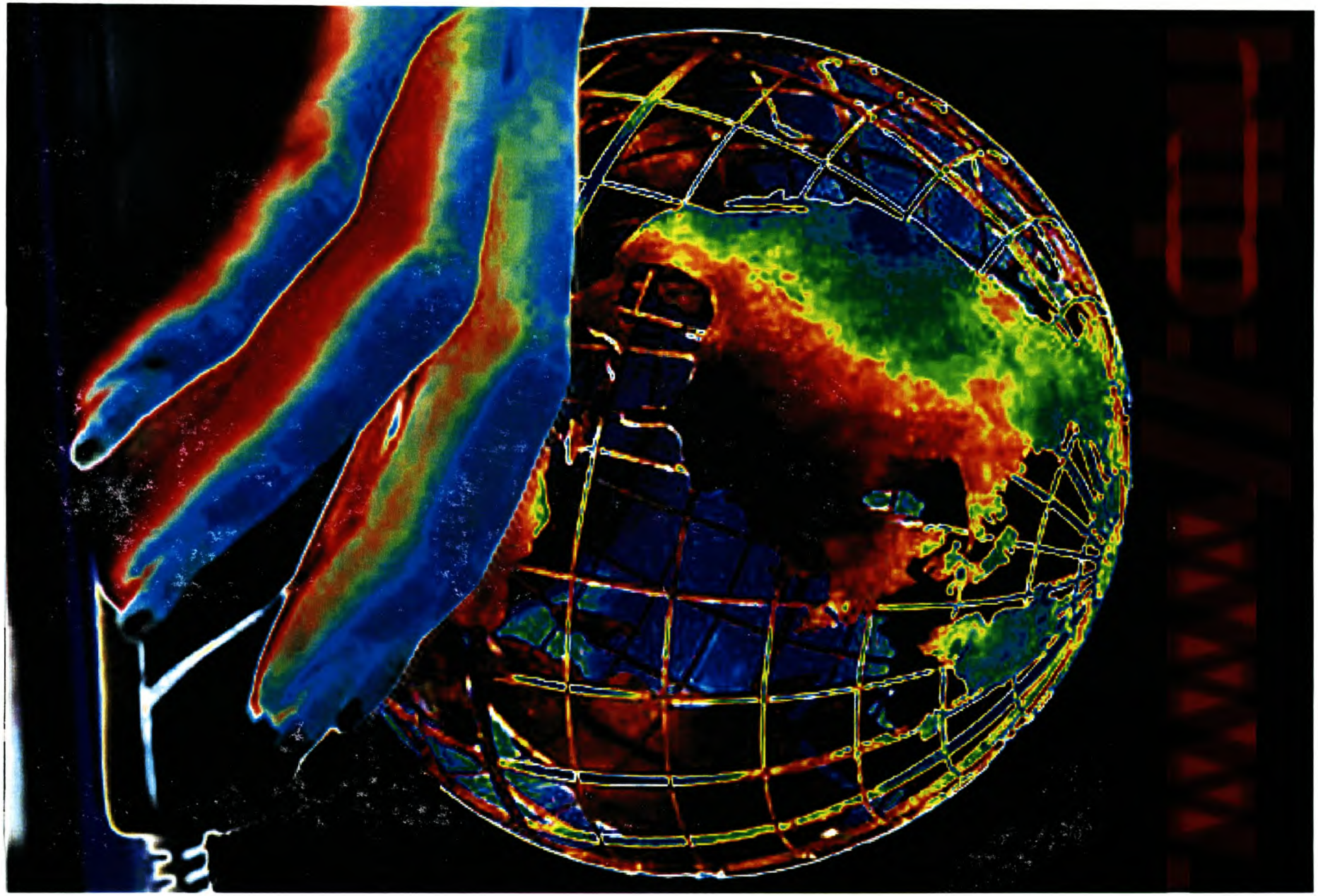
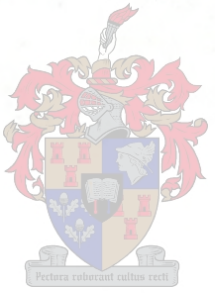
Grafika: Lezél Amoraal



INTERNET-REGULERING IN SUID-AFRIKA: STAAT OF INTERNASIONAAL?

Lezél Amoraal



Werkstuk ingelewer ter gedeeltelike voldoening aan die vereistes vir die graad MPhil (Joernalistiek) aan die Universiteit van Stellenbosch

Studieleier:
Prof L Rabe

April 2003

Stellenbosch University http://scholar.sun.ac.za

Ek, die ondergetekende, verklaar hiermee dat die werk in herdie werkstuk vervat, my eie oorspronklike werk is en dat ek dit nie vantevore in die geheel of gedeeltelik by enige universiteit ter verkryging van 'n graad voorgelê het nie.

Handtekening

Datum

Stellenbosch University http://scholar.sun.ac.za

ABSTRAK

Die Internet het al so deel van rekenaargebruikers se alledaagse bestaan geword dat dit soms wil voorkom asof dit maar nog altyd daar was.

Die Internet met sy unieke grense – of sy gebrek aan grense – plaas 'n groot las op geografies gebaseerde regstelsels. Regulering wat spesifiek vir die Internet ontwerp is, is 'n noodsaaklikheid, aangesien byna elke aspek van die reg deur die Internet uitgedaag word en baie regsraamwerke onvoldoende is om die Internet te hanteer.

Wat die regulering van die Internet verder kompliseer, is dat daar nie een spesifieke organisasie, onderneming of regering is aan wie die Internet behoort nie. Individue en organisasies het regte tot die webwerwe wat hulle op die Internet besit, maar daar is nie eienaarskap van die Internet in sy geheel nie.

Die ontwikkeling van die Internet in Suid-Afirka het tydens 'n moeilike tydperk in die Suid-Afrikaanse geskiedenis plaasgevind. Die apartheidsera het die aanvanklike ontwikkeling en groei van die Internet in Suid-Afrika beperk. Verskeie bestaande Suid-Afrikaanse wetgewing is deels aangepas om die Internet te akkommodeer, maar die regering het nooit besef wat die werklike impak van die Internet sou wees nie en het gevolglik re-aktief te werk gegaan wanneer dit by die regulering van die Internet gekom het. In 2002 het Suid-Afrika se Elektroniese Kommunikasie en Transaksies Wet 25 van 2002 in werking getree.

Die regulering van die fisieke komponente van die Internet is tot 'n mate as gevolg van sy fisieke teenwoordigheid deur blote toeval, gereguleer. Dit is omdat die ruggraat van die Internet nie oorspronklik vir die Internet geskep is nie, maar vir die telefoon.

Daar bestaan verskeie wetgewende Internet-organisasies wat onder meer verantwoordelik is vir die tegniese standaarde van die Internet, dispuutresolusie en wat oor die algemeen aan die belange van die Internet-gemeenskap wil voldoen.

Verskeie internasionale konvensies reguleer spesifieke aspekte van die Internet soos kopiereg, intellektuele eiendomsreg, domeinname en handelsmerke en kubermisdaad. Die internasionale konvensies en verdrae is 'n belangrike stap in die rigting van gestandaardiseerde regulering. Tog skep die grenslose omstandighede van die Internet probleme rondom jurisdiksie in die kuberruim.

Stellenbosch University http://scholar.sun.ac.za

ABSTRACT

The Internet has become such an integral part of computer users' daily existence that it seems as if it has always been there.

The Internet with its unique borders – or lack of borders – places an enormous burden on geographically based legal systems. Regulation, that has specifically been designed for the Internet, is a necessity because virtually every aspect of the law is challenged by the Internet and that many legal frameworks are inadequate to deal with the Internet.

The other aspect which complicates the Internet even more, is that there is no specific organisation, business or government to whom the Internet belongs. Individuals and organisations have rights to the web pages that they own on the Internet, but there is no ownership of the Internet in its entirety.

The development of the Internet in South Africa took place during a difficult time in the country's history. The apartheid era initially limited the growth of the Internet. Much of the existing legislation in South Africa has been partially adapted to accommodate the Internet, but the government could not envisage what the actual impact of the Internet would be and consequently they reacted when it came to the regulation of the Internet. In 2002 the Electronic Communication and Transaction Act 25 of 2002 came into operation.

In fact, the physical component of the Internet has already been regulated to a degree by the pure coincidence as a result of its physical presence. This is because the backbone of the Internet had not originally been created by the Internet, but by the telephone.

There are a number of legislative Internet-organisations that are, among others, responsible for the technical standards of the Internet, dispute resolutions and in general what is important for the Internet community.

Various international conventions regulate specific aspects of the Internet such as copyright, intellectual property rights, domain names, trademarks and cyber crime. The international conventions and agreements are an important step in the direction of standardised regulation. However, the lack of borders creates problems surrounding jurisdiction of the cyber space.

Stellenbosch University http://scholar.sun.ac.za

INHOUDSOPGAWE

Stellenbosch University http://scholar.sun.ac.za

Stellenbosch University http://scholar.sun.ac.za

Bylaes 117

Bronnelys

Stellenbosch University http://scholar.sun.ac.za

LYS VAN TABELLE

Hoofstuk 1: Inleiding

Hoofstuk 3: Ontwikkeling van die Internet

Hoofstuk 4: Die Internet in Suid-Afrika

Stellenbosch University http://scholar.sun.ac.za

Hoofstuk 5: Internet-regulering

Stellenbosch University http://scholar.sun.ac.za

BEDANKINGS

Eerstens, aan my promotor:

- Prof. Lizette Rabe: vir al die moed inpraat, hulp en al die rooimerke. Ek het so baie geleer.

Tweedens, aan my familie:

- Ma: vir al die ure van deurlees, ondersteuning
- Pa: vir die ISDN Internet-konneksie by die huis, die rekenaar en al die papier wat ek gebruik het.
- Jolanda: vir die ondersteunende selfoongesprekke. Jou beurt kom nog.
- Willemjan: vir die laataand video's wat ons gekyk het as ek 'n "break" nodig gehad het.
- Al ons diere: Snoepie en Melba (honde) omdat julle nie een van my papiere opgeëet het nie en Wolfie (kat) omdat jy darem ligvoets oor al my navorsing kon stap en niks verwoes het nie.

En laastens, aan my vriendinne:

- Amanda, Babsie en Mandie: julle weet waarvoor.

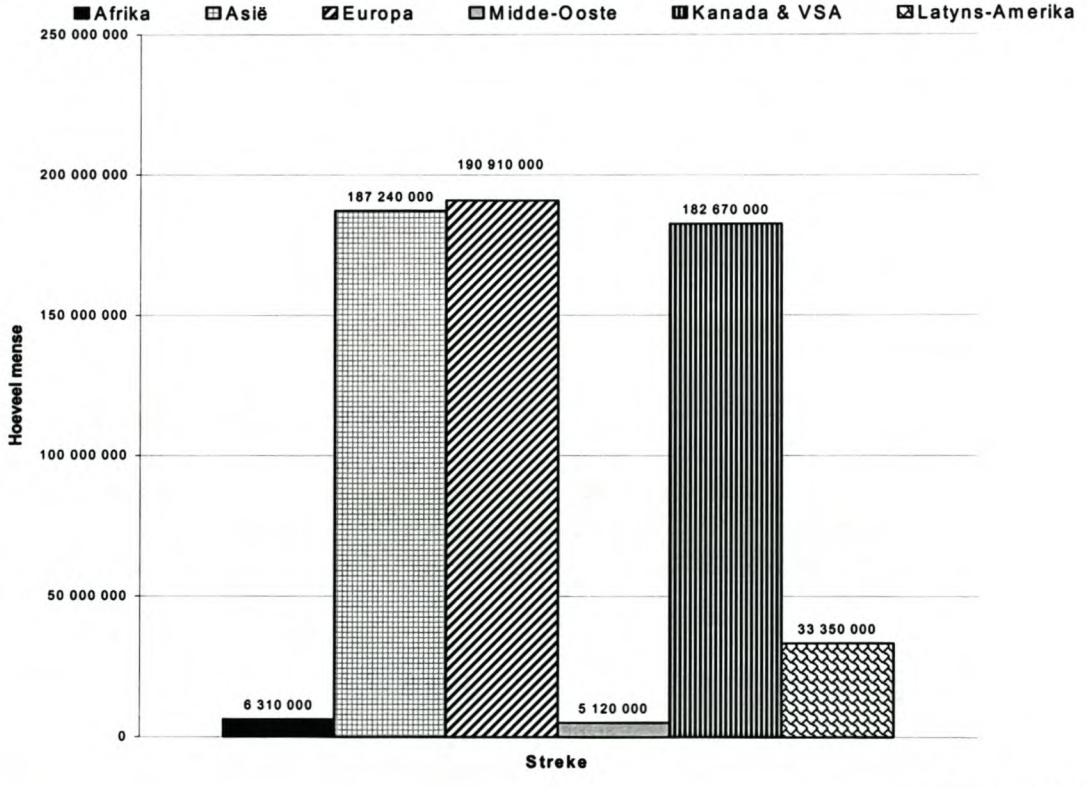
Stellenbosch University http://scholar.sun.ac.za

HOOFSTUK 1
INLEIDING

1.1 Agtergrond

Die Internet het al so deel van rekenaargebruikers se alledaagse bestaan geword dat dit soms wil voorkom asof dit maar nog altyd daar was (Leiner et al, 2000:1). Teen September 2002 was daar ongeveer 605 miljoen mense wêreldwyd wat die Internet gebruik. Die grootste gedeelte is mense in Eerste Wêreldlande soos in Tabel 1.1 gesien kan word ("How many online", 2002:1).

TABEL 1.1: Aantal mense aanlyn (Sept. 2002)

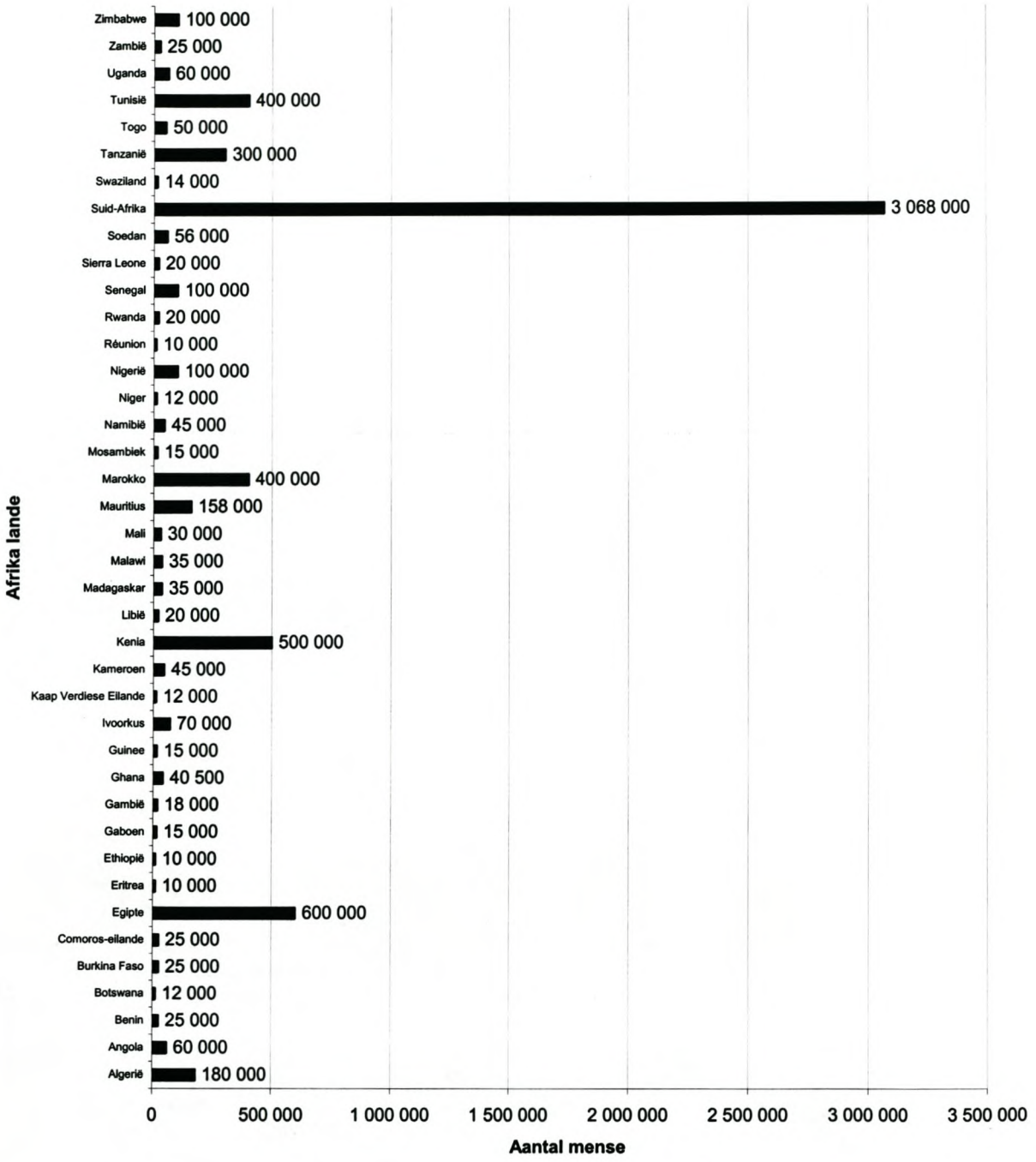


Bron: www.nua.ie

Afrika is as deel van die Derde Wêreld nie goed verteenwoordig in die tabel nie, met die uitsondering van Suid-Afrika ("How many online", 2002:1). Volgens 'n onlangse studie (sien Tabel 1.2) deur www.nua.ie, 'n webwerf wat Internet-tendense en statistieke monitor, was daar teen die einde van 2001 ongeveer 3 miljoen Suid-Afrikaners aanlyn ("World Wide Wox: More South Africans", 2002).

Stellenbosch University http://scholar.sun.ac.za

TABEL 1.2: Aantal mense aanlyn in Afrika (Des 2001)



Bron: www.nua.ie

Tabel 1.2 bevat slegs dié Afrika-lande waar 10 000 of meer mense van die land teen Desember 2001 aanlyn was. In Tabel 1.3 verskyn die volledige lys van Afrika-lande soos deur 'n onlangse studie van www.nua.ie aangeteken. In dié tabel word die hoeveelheid mense gelys en watter persentasie die aantal mense aanlyn van die bevolking vorm. Dis interessant as daar na die

Stellenbosch University http://scholar.sun.ac.za

persentasie van die bevolking gekyk word dat die Seychelles met 11% die beste vertoon, met Suid-Afrika in die tweede plek met 7%. Daar moet egter in gedagte gehou word dat slegs 9 000 van die Seychelles se bevolking aanlyn is, in vergelyking met die 3 068 00 van Suid-Afrika.

TABEL 1.3: Aantal mense aanlyn in Afrika (Des 2001)

LAND	Hoeveelheid	% van bevolking	LAND	Hoeveelheid	% van bevolking
Algerië	180,000	0.57%	Malawi	35,000	0.33%
Angola	60,000	0.57%	Mali	30,000	0.26%
Benin	25,000	0.37%	Mauritanië	7,000	0.25%
Botswana	12,000	0.78%	Mauritius	158,000	0.13%
Burkina Faso	25,000	0.2%	Marokko	400,000	1.28%
Burundi	6,000	0.09%	Mosambiek	15,000	0.08%
Comoros-eilande	25,000	0.41%	Namibië	45,000	2.47%
Djiboeti	3,300	0.70%	Niger	12,000	0.11%
Egipte	600,000	0.85%	Nigerië	100,000	0.08%
Ekwatoriaal-Guinee	900	0.22%	Principe	9,000	5.28%
Eritrea	10,000	0.22%	Réunion	10,000	1.39%
Ethiopië	10,000	0.02%	Rwanda	20,000	0.27%
Gaboen	15,000	1.24%	Senegal	100,000	0.94%
Gambië	18,000	1.24%	Sentraal Afrikaanse Republiek	2,000	0.05%
Ghana	40,500	0.2%	Seychelles	9,000	11.24%
Guinee	15,000	0.19%	Sierra Leone	20,000	0.38%
Guinee Bissau	4,000	0.3%	Soedan	56,000	0.15%
Ivoorkus	70,000	0.13%	Somalië	200	-
Kaap Verdiese Eilande	12,000	2.94%	Suid-Afrika	3,068,000	7.03%
Kameroen	45,000	0.28%	Swaziland	14,000	1.25%
Kenia	500,000	1.61%	Tanzanië	300,000	0.81%
Kongo-Brazzaville	500	0.02%	Togo	50,000	0.95%
Kongo-Kinshasa	6,000	0.01%	Tsjad	4,000	0.040%
Lesotho	5,000	0.23%	Tunisië	400,000	4.08%
Liberië	300	0.01%	Uganda	60,000	0.24%
Libië	20,000	0.24%	Zambië	25,000	0.25%
Madagaskar	35,000	0.21%	Zimbabwe	100,000	0.88%

Bron: www.nua.ie

Die meeste mense wat wêreldwyd Internet-toegang het, maak gereeld daarvan gebruik. Dié gebruikers verteenwoordig alle vlakke en ouderdomsgroepe van die samelewing. Sommige gebruik die Internet as 'n hulpmiddel om akademiese navorsing te doen, ander beskou dit as 'n geriefliker alternatief vir 'n inkopiesentrum, vir party is dit 'n vermaaklikheidsentrum of 'n bron van inligting of nuus, terwyl sommiges weer e-pos gebruik om vinnig en goedkoop met mense regoor die wêreld te kommunikeer (Leiner et al., 2000:12).

Stellenbosch University http://scholar.sun.ac.za

'n Konstante gevaar vir Internetdiensverskaffers (IDV's) en operateurs van bulletinborde en nuusgroepe is om vir laster gedagvaar te word. Daar is elke dag honderde boodskappe wat die grense van vryheid van spraak en laster oorsteek. Elke nuusgroep is 'n openbare forum waar die Internetgebruiker enige boodskappe kan lees of pos (Buys, 2001:329).

Joe Gutnick, 'n goudmagnaat, wat die Dow Jones se publikasie *Barrons* dagvaar vir laster oor bewerings in 'n artikel op die Internet, het 'n Australiese hooggeregshof gevra of sy saak ingevolge Australiese wetgewing verhoor kan word. In 'n onlangse belangrike uitspraak het die hooggeregshof in Australië beslis dat beweerde laster wat in Amerika gepleeg is, nou in Australië vervolg kan word. Oortreders word gewoonlik in hul eie land aan die hand van plaaslike wetgewing vervolg.

Dié uitspraak sal probleme vir alle Internet-uitgewers verskaf, aangesien die Australiese-uitspraak nou in beginsel van elke uitgewer verwag om die inhoud van sy webwerf so saam te stel dat dit aan honderde lande wat op die Internet verteenwoordig is, se regstelsels sal voldoen (Rademeyer, 2003:8).

Daar is 'n paar aspekte wat uniek is tot die Internet wat dit onderskei van ander media waardeur lasterlike inhoud gepubliseer kan word en wat tot die herondersoek van die huidige reëls oor laster gelei het (Buys, 2001:329).

Een vraagstuk is: Watter rol speel IDV's in die inhoud van webblaaie wat deur sy kliënte/werkgewers op die Internet gepubliseer word?

Nog 'n vraag wat beantwoord moet word is: Moet IDV's ook 'n regulerende funksie ook hê?

Die geskiedenis van Internet-regulering begin by APRANET[1] toe die Amerikaanse regering beheer daaroor gehad het. Vandag het die Amerikaanse regering egter nie meer alleenreg oor die uitvloeisel van APRANET, nl. die Internet, nie (Niemczyk, 1999:1).

Daar is twee beleidsvrae om oor na te dink.

Die eerste is 'n normatiewe vraag: Moet die Internet gereguleer word?

Wanneer die eerste vraag beantwoord is, en daar besluit is dat die Internet wel gereguleer moet word en daar 'n konsensus is oor watter aktiwiteite gereguleer moet word, bring dit die tweede vraag na vore: Hoe kan die Internet effektief gereguleer word? (Niemczyk, 1999:1).

Ook Suid-Afrika moes sy wetgewing aanpas om te verseker dat die Internet effektief gereguleer word. Die nuwe Elektroniese Kommunikasie en Transaksies Wet van 2002, glo kenners, is die eerste stap in die regte rigting vir Suid-Afrikaanse Internet-regulering (Vegter & De Wet, 2002:27).

---

[1] APRANET (Advanced Research Projects Agency Network): Die voorloper van die Internet wat in die laat 1960's en begin 70's ontwikkel is deur die Amerikaanse Departement van Verdediging.

Stellenbosch University http://scholar.sun.ac.za

Sekere Suid-Afrikaanse webwerwe word gereeld deur Internet-gebruikers in Suid-Afrika en oor die res van die wêreld gebruik. Een van dié webwerwe was M-Web Afrikaans[2], wie se gespreksforum ongeveer twee weke lank deur 'n ander Afrikaanse webtuiste, www.watkykjy.co.za, lam gelê is deur sinlose boodskappe en skaamtelose reklame vir www.watkykjy.co.za. Die oorsaak van die aanval op M-Web Afrikaans het geblyk dat dit gaan oor die gebruik van "Ou Koeie" (verwysend na die idioom: "Moenie ou koeie uit die sloot grawe nie") as verwysing na die argief van die twee webwerwe, wkj? en M-Web Afrikaans. Albei webwerwe het die naam "Ou Koeie" as skakel na hul argiewe. M-Web Afrikaans het wel eerste "Ou Koeie" gebruik, maar wkj? het toevallig ook op "Ou Koeie" besluit sonder dat hulle bewus was van M-Web Afrikaans se gebruik daarvan ("wkj? en M-Web Afrikaans", 2001:1).

Ná dié gebeurtenis wil 'n mens weet of daar nie stappe teen www.watkykjy.co.za geneem kon word nie. Is daar wetgewing in Suid-Afrika wat hul optrede verbied?

'n Ander voorval wat in Januarie 2002 ter sprake was, het voorgekom op die Suid-Afrikaanse nuus-webtuiste www.news24.com. Dit het gegaan oor die Amerikaner Vern Six wat ná 'n onbevredigende SAL-vlug na Suid-Afrika 'n webwerf www.neverflysaa.com begin het (SAPA, 2002:1). Sedert die bestaan van www.neverflysaa.com het die webwerf blykbaar al meer as 6,5 miljoen bladindrukke ("hits") gehad en meer as 81 000 intekenare op sy poslys (Six, 2002:1).

Hoe gebeur dit dat 'n skynbaar lasterlike webwerf soos www.neverflysaa.com op die Internet toegelaat word?

Die antwoord is eenvoudig. Mnr. Six van Austin, Texas het die domeinnaam www.neverflysaa.com by www.register.com geregistreer.

SAL het op 9 April 2002 'n klag by die Amerikaanse Nasionale Arbitrasie Forum gelê en gevra dat die domeinnaam www.neverflysaa.com aan SAL oorgegee moet word. SAL het egter die saak op 30 Mei 2002 verloor ("National Arbitration Forum", 2002:3).

Die verwoestingswerk van die kuberkraker r00t3rs vanaf 16 Oktober 2002 in Suid-Afrika is die ergste sedert die ontstaan van die Internet, berig *Die Burger* (Ferreira, 2002:1).

Volgens Reinhardt Buys van Buys-prokureurs fokus die kuberkraker op Suid-Afrikaanse webwerwe wat op die Windows NT-stelsel gebou is en slaan toe op 'n swak plek in die stelsel om toegang tot die webwerf te kry en dit heeltemal te verwoes. As dié kuberkraker aangekeer word, sal dit die eerste kuberkraker-saak wees wat ingevolge Suid-Afrika se nuwe Internet- en e-handelswetgewing verhoor sal word (Ferreira, 2002:1).

[2] M-Web Afrikaans is in Julie 2001 deur News24 oorgeneem. News24 vorm deel van Naspers se e-madia 24.

Stellenbosch University http://scholar.sun.ac.za

1.2 Probleemstelling

Die hoofdoel van die studie is om vas te stel of Internet-regulering in Suid-Afrika slegs deur die staat/regering behartig moet word. Die studie poog ook om vas te stel of dit nie moontlik is dat selfregulering en internasionale regulering van die Internet, staatsregulering in die toekoms kan vervang nie.

Daar is sekere kernvrae wat die studie moet beantwoord:

1. Hoe het die Internet ontstaan?
2. Aan wie behoort die Internet? (Insluitende 'n definisie van die Internet.)
3. Wie gebruik die Internet?
4. Wie is die Internet-organisasies en rolspelers in die wêreld en Suid-Afrika?
5. Wat is Internet-wetgewing en hoekom is dit so belangrik?
6. Hoe word Internet-wetgewing in Suid-Afrika hanteer?
7. Wie behoort die Internet in Suid-Afrika en die res van die wêreld te reguleer?
8. Wat is identiteitsdiefstal en wat kan gedoen word as iemand 'n slagoffer van identiteitsdiefstal is?
9. Kan Internet-diensverskaffers verantwoordelik gehou word vir inhoud wat deur hulle kliënte op die Internet geplaas word?
10. Wat is netiket?
11. Hoe word kopiereg op die Internet beskerm?
12. Watter probleme skep domeinname en handelsmerke vir die Internet?
13. Hoe word die toekenning van domeinname gereguleer?
14. Wat word gedoen om kuberplakkery te bekamp?
15. Watter stappe kan gedoen word om te keer dat iemand anders jou domeinnaam en handelsmerk gebruik?
16. Wat is kubermisdaad en hoe word dit gereguleer?
17. Wat behels die nuwe Elektroniese Kommunikasie en Transaksies Wet van 2002?

1.3 Raamwerk van studie

Die studie kyk nie na die voorkoms van plagiaat op die Internet nie, aangesien dit 'n studie op sigself vereis.

Die literatuurstudie word in Hoofstuk 2 bespreek. Verskeie bronne is geraadpleeg wat as agtergrond en riglyn vir dié studie oor Internet-regulering in Suid-Afrika dien. Die bronne word kortliks bespreek asook die gevolgtrekkings wat die bronne gemaak het.

Stellenbosch University http://scholar.sun.ac.za

In Hoofstuk 3 sal die ontstaan en ontwikkeling van die Internet bespreek word. Die kernvraag of die Internet aan iemand behoort, wat in die Probleemstelling uiteengesit is, word beantwoord. Daar word ook na die demografie van Internet-gebruikers gekyk deur verskillende opnames wat deur webwerwe op die Internet gedoen is.

Hoofstuk 4 handel oor die Internet in Suid-Afrika en in besonder oor die geskiedenis en ontwikkeling van die Internet in die land. Die demografie van Suid-Afrika se Internet-gebruikers word ook kortliks hier bespreek.

In Hoofstuk 5 word Internet-regulering in die algemeen bespreek. Die Internet kan deur sy fisieke struktuur (die Internet-ruggraat) en sy inhoud onderskei word. Dit is nodig vir die regulering van die Internet. Die verskillende Internet-rolspelers en belangrike Internet-organisasies beïnvloed die regulering van die Internet – nie net deur hul verskillende beleide nie, maar ook deur hul optrede en die tipe funksie wat hulle verrig. In dié hoofstuk word daar op drie belangrike reguleringsaspekte van die Internet gefokus, naamlik kopiereg, handelsmerke en domeinname en kubermisdaad.

Hoofstuk 6 handel oor Internet-regulering in Suid-Afrika, die Internet-rolspelers in die land en ook oor die Elektroniese Kommunikasie en Transaksies Wet van 2002. Daar sal aan die einde van die hoofstuk ook 'n kort bespreking wees oor hoe kopiereg, handelsmerke en domeinname en kubermisdaad in Suid-Afrika gereguleer word. Drie gevallestudies word kortliks bespreek en hoe kopiereg, handelsmerke en domeinname en kubermisdaad daarop betrekking het. Die gevallestudies wat bespreek word is M-Web Afrikaans en die Afrikaanse webwerf www.watkykjy.co.za; SAL se webwerf www.flysaa.com en Vern Six se www.neverflysaa.com en die kuberkraker r00t3rs se manewales op Suid-Afrikaanse webwerwe.

Die Gevolgtrekking van dié studie word in Hoofstuk 7 bespreek. Die kernvraag van die studie of Internet-regulering in Suid-Afrika slegs deur die staat/regering behartig moet word en of dit moontlik is dat selfregulering en internasionale regulering van die Internet staatsregulering kan vervang, sal beantwoord word.

Stellenbosch University http://scholar.sun.ac.za

HOOFSTUK 2
LITERATUURSTUDIE

Hoekom is Internet-regulering nodig? Wat is netiket? Dit is van die kernvrae, wat in Hoofstuk 1 by 1.2 gelys is, wat in dié hoofstuk bespreek word. Daar sal onder meer gekyk word na die ontwikkeling van massa-kommunikasie en hoe die Internet deel daarvan vorm. Aan die einde van die hoofstuk behoort 'n mens 'n redelike duidelike agtergrond te hê van watter tipe regulering daar vir die Internet bestaan en hoe die toekoms van Internet-regulering daarna uitsien.

Verskeie internasionale studies oor die regulering van die Internet en die moontlike internasionale regulering onder een sentrale ligaam is al gedoen. Die meeste van die studies kyk na huidige regulering wat beskikbaar is en maak voorstelle vir 'n nuwe model van regulering. As 'n mens die soekterm "studies Internet regulation" op die soek-enjin Google intik, is daar 3 410 soekresultate. Daar was onder meer Graham J.H. Smith se studie "Internet Law and Regulation" wat in 1996 geskryf is, wat handel oor Internet-regulering in die Verenigde Koninkryk. Gedeeltes van die inligting is reeds verouderd en slegs van toepassing op die Verenigde Koninkryk (Smith, 1996:1). Ook Henry H Perritt Jr se studie "Law and The Information Superhighway" wat in 1996 gepubliseer is, bevat verouderde inligting (Perritt, 1996:1).

In dié hoofstuk sal Stephen Baker se artikel "Taming the Wild, Wild Web: Without strong laws, the Net's growth will be stunted" wat in *Business Week* (1999) verskyn het, bespreek word en daar sal na Jason Niemczyk se studie oor Internet-regulering gekyk word. Baker se studie bied 'n kort oorsig oor hoekom regulering noodsaaklik is en watter tipes regulering beskikbaar is. A.M. Froomkin se studie "An Introduction to the 'governance' of the Internet" (1995) konsentreer meestal op die self-regulering van die Internet. Niemczyk se studie word bespreek omdat dit redelik in detail uiteensit watter tipe regulering beskikbaar is, wat die sterk- en swakpunte van die verskillende tipes regulering is en wat die toekoms van Internet-regulering moet wees. Die studies wat in die hoofstuk bespreek word, is steeds van toepassing, bevat nie verouderde inligting nie en bespreek Internet-regulering soos dit wêreldwyd benader word.

2.1 Die ontwikkeling van massa-kommunikasie

Dit wil voorkom asof die Internet 'n vormlose virtuele netwerk met terminale en diensrekenaars is wat in geen spesifieke volgorde versprei en lukraak oor die wêreld verbind is. Inligting, hetsy teks, beelde, klank, video of ander datasoorte kan van enige plek na enige ander plek opgeroep of

Stellenbosch University http://scholar.sun.ac.za

gestuur word deur slegs die kliek van 'n muisknoppie. Dis egter nie waar die Internet se grootste geleenthede lê nie. Die Internet moet eerder as 'n sosiale fenomeen gesien word.

In werklikheid is die Internet nog 'n kommunikasie-medium wat help om die "global village" in staat te stel om tot sy volle potensiaal te funksioneer (Opperman, 2000:1). Die "global village"-idee is afkomstig van Marshall McLuhan wat die eerste persoon was wat in die 1960's dié populêre konsep begin gebruik het en wat die sosiale effek van die "global village" voorspel het. Sedert sy insigte het die wyse waarop mense aan die media, tegnologie en kommunikasie dink, verander. Hy het die frase "global village" gekies om sy konsep van 'n elekroniese senuweestelsel wat vinnig besig is om die wêreld te integreer, te verwoord. Dié "global village" veroorsaak dat gebeure wat aan die een kant van die wêreld gebeur direk op dieselfde tyd aan die aan die anderkant van die wêreld ervaar kan word (Altshull, 1990:337-343).

Dit was eers in die 15de eeu toe die Duitse goudsmid Johann Gutenberg die beweegbare lettertipe ("moveable type") ontdek het, dat die druk-industrie ontwikkel het (Diederichs & De Beer, 1998:87). Die Gutenberg-drukkery het veroorsaak dat die beskikbaarheid van inligting nie meer beperk was tot slegs die Rooms-Katolieke Kerk en adellikes nie. Dit het ook vir die ander klasse in die Europese samelewing beskikbaar geword. Die Gutenberg-drukkery het die fondamente gelê vir die eerste massa-medium, nl. koerante.

In die 19de eeu is kommunikasie deur verskeie media bepaal. Drukmedia, veral koerante, is ondersteun deur die telegraaf en telefoon. Met die koms van radio, film en televisie in die 20ste eeu het massa-kommunikasie geweldig ontwikkel. Op die oomblik is 'n "inligtingsgemeenskap" besig om te ontwikkel. Met die hulp van digitale kommunikasie word tegnologiese netwerke tot stand gebring waarbinne geïntegreerde multi-media applikasies moontlik is (Temme, 1997:2).

In die "global village" kan enige individu of organisasie 'n verkoper of verbruiker, 'n uitgewer of intekenaar wees met byna geen agting vir nasionale wette of grense nie. Vervaardigers, uitgewers, kliënte en vriende is almal net aan die oorkant van die digitale straat, selfs al is hulle duisende kilometers ver. Dit bring kommersiële-, sosiale-, morele-, fiskale-, politiese- en regsimplikasies na vore (Opperman, 2000:2).

Tog is daar die Minder Ontwikkelde Lande (Less Developed Countries) wat konstant sukkel om tred te hou met die tegnologiese ontwikkelings. Hulle Internet-toegang is beperk weens hul bykans primitiewe netwerk struktuur (Moses. 1999:1).

Die AISI (African Informations Society Initiative) is een van die belangrikste stappe wat geneem is om die "digitale gaping" te oorbrug. Die doel van AISI is "die verkryging van 'n volhoubare inligtingsgemeenskap in Afrika teen 2010". Margot Moses vra in haar studie *Internet Demographics* (1999) hoe dit vir Afrika moontlik gaan wees om deel van die "global village" te word wanneer hulle ook kostes moet minimaliseer.

UNIVERSITEIT STELLENBOSCH

Stellenbosch University http://scholar.sun.ac.za

2.2 Hoekom is Internet-regulering nodig?

'n Franse hof se onlangse mylpaaluitspraak is 'n goeie voorbeeld van watter implikasies die Internet inhou. Die Franse regter Jean-Jacques Gomez het die VSA gebaseerde portaal Yahoo! verplig om Franse Internet-gebruikers van 'n veiling wat Nazi-memorabilia verkoop, te blokkeer. Dit is onwettig in Frankryk om rassistiese materiaal ten toon te stel of te verkoop. Yahoo! is drie maande gegee om 'n manier te kry om te keer dat Franse gebruikers die webblaaie op actions.yahoo.com kan oopmaak (Barlow, 2001:1).

Bykans elke aspek van die reg word deur die Internet uitgedaag en baie regsraamwerke is onvoldoende om die Internet te hanteer (Opperman, 2000:3). Die Internet se unieke grense - of sy gebrek aan grense - plaas 'n groot las op tradisioneel geografies gebaseerde regstelsels.

Internasionale regstoepassing raak nog meer kompleks. Misdade wat in een land plaasvind, kan nou reg oor die wêreld plaasvind. Selfs nadat besluit is watter wet om toe te pas, en daar jurisdiksie oor die beskuldigde verkry is, word die meeste lande se vermoë om wetgewing toe te pas op 'n oortreding wat as 'n misdaad onder hul wetgewing beskou word, beïnvloed deur die bepaling van die *locus delicti*, die plek van oortreding (Niemczyk, 1999:2).

Ongekende tegnologiese vooruitgang maak die definiëring van regskonsepte en misdade moeilik. Wat lande deesdae tegnologies beperk, mag dalk oor vyf jaar nie meer beperkend wees nie. Terwyl die Internet 'n belangrike deel vorm van kommunikasie, moet lande tegnologies vooruitgaan om in die internasionale mark mededingend te bly. Om wette in werking te stel wat tegnologie beheer, kan 'n direkte invloed op ander lande hê (Niemczyk, 1999:2).

Die meeste lande voel die huidige tegnologie kan nie die verskillende beginsels oor vryheid van spraak op die Internet akkommodeer nie. Nie alle lande definieer vryheid van spraak op dieselfde manier nie. Selfs binne dieselfde land, binne 'n homogene taalgroep, is die idee van vryheid van spraak nie duidelik nie. Hoe dit ook al sy, terwyl die definisie van vryheid van spraak betwis word, moet mens verstaan dat taalgrense gewoonlik dié konflikte op die Internet kan oplos. Taalgrense kan dien as 'n plaasvervanger vir die geografiese grense wat die Internet nodig het (Niemczyk, 1999:2).

Die ontwikkeling van die Internet is deur baie gesien as die begin van die einde van intellektuele eiendomsreg. Die oorspronklike gebruikers van die Internet was meestal regerings en universiteite. Hulle het nie die Internet gebruik as 'n bron van inkomste nie, maar om inligting te bekom en te versprei. Die Internet was 'n gratis kommunikasie-medium wat mense toegelaat het om hul opinies met die hele wêreld te deel. Dit het ook perfekte, goedkoop reproduksies van enige inligting of werk op 'n ongeëwenaarde skaal moontlik gemaak (De Villiers, 2001:37).

Stellenbosch University http://scholar.sun.ac.za

Wêreldwye deelname aan die Internet is 'n relatiewe nuwe fenomeen, wat danksy die kommersialisering van die Internet moontlik gemaak is. Dit sluit in:

1. die groei en sukses van Internetdiensverskaffers,
2. die ontwikkeling van Internetsagteware en
3. uiteindelik die ontwikkeling van kommersiële webwerwe.

Dit het verseker dat die algemene publiek se toegang tot die Internet bekostigbaar is en nie tegnies gekompliseerd nie (Niemczyk, 1999:3).

Dit was onvermydelik dat die ekonomiese potensiaal van die Internet deur groot ondernemings raakgesien sou word. Regulering van die Internet moes noodwendig volg.

Die probleem met regulering is die internasionale karakter van die Internet. Intellektuele eiendomsregulering is nasionaal gebaseerd. Elke land het sy eie wette wat kopiereg, handelsmerke, patente, ontwerpe en handelsname reguleer, maar enigeen wat op die Internet publiseer, kan intellektuele eiendomsreg of enige ander regte of wette op enige plek in die wêreld oortree. Regerings sal daarom gedwing word om weens die aard van die Internet in die toekoms wetgewing te standaardiseer (De Villiers, 2000:37).

Die koms van die Internet het onsekerheid geskep oor hoe huidige wette toegepas moet word.

Dié revolusionêre verandering in tegnologie het egter 'n meer fundamentele onsekerheid veroorsaak oor hoe individue op die Internet te werk sal gaan.

2.3 Netiket

Op die onbekende terrein van die Internet is sosiale en kulturele norme nog nie vasgestel nie. Daar is nie 'n absolute afwesigheid van sosiale gebruike op die Internet nie - Internet-burgers praat gereeld van "net-etiket" of "netiket". Volgens Niemczyk (1999) is Internet-burgers tans besig om gedragsnorme en verwagtinge rakende Internet-verhoudings te skep wat verby eenvoudige netiket beweeg.

> "Netiket skryf slegs individuele gedrag voor, dit los nie konflikte op wat geskep word deur diegene wat buite die verwagte sosiale gedrag optree nie. Verder is netiket nie by magte om ernstiger oortredings en verbreking van openbare standaarde soos inligtingsdiefstal en kinderpornografie te hanteer nie" (Niemczyk, 1999:6).

Die interessante aspek van netiket is dat dit die begin beteken van standaarde wat ontwerp is om die gedrag op die Internet te reguleer. "Netiket beïnvloed die manier hoe ons dink oor gedrag op die Internet" (Niemczyk, 1999:6).

Stellenbosch University http://scholar.sun.ac.za

Die bestaan van 'n aanlyn-moraliteit verwyder nie die noodsaaklikheid van wetgewing wat spesifiek sekere morele standaarde aanspreek en afdwing nie. "Die Internet het wette nodig net soos ons gemeenskap wette nodig het om ons sosiale waardes en kontrakte af te dwing" (Niemczyk, 1999:6).

2.4 Internet-reguleringstudies

Volgens Stephen Baker se artikel "Taming the Wild, Wild Web: Without strong laws, the Net's growth wil be stunted" (1999) in *Business Week* het ondernemings geen ander keuse nie as om met hul eie stel reëls vorendag te kom as hulle hul eiendomsregte wil beskerm en gebruikers veiliger op die Internet wil laat voel.

Baker glo die Internet ontwikkel twee parallelle en soms mededingende reguleringstelsels. Die sukses van die twee stelsels - openbaar en privaat - sal bepaal hoe magtig die Internet sal word (Baker, 1999:93-94). Die openbare stelsel is regulering wat deur verskillende Internet-organisasies en lande se regstelsels toegepas word, terwyl die private stelsel op selfregulering deur individue dui (Niemczyk, 1999:9).

Die probleem is egter dat die opstel en aanvaarding van Internetwetgewing en reguleringstelsels tyd neem. Wetgewing wat in twee jaar afgehandel word, word as betreklik vinnig beskou. Ongelukkig is twee jaar in Internet-terme meer soos twee eeue, waarin verskeie tegnologiese deurbrake sou plaasvind en die wetgewing reeds as verouderd beskou kan word (Baker, 1999:94).

Niemczyk se studie *International Internet: A look inside* (1999) bespreek private regulering van die Internet deur individue, soewereine state se regulering deur die kombinering van die Internet met huidige regstelsels en stel die moontlikheid voor van 'n "kuberregering" wat dié internasionale organisasie sal wees wat die Internet sal reguleer.

2.4.1 Selfregulering

Selfregulering vind plaas wanneer private individue hoogs suksesvolle strategieë soos self-help, kollektiewe aksie en private kontrakte implementeer om hul besorgdheid oor die Internet te hanteer. Private individue sal voortgaan om die metodes te gebruik selfs nadat die reguleringsgaping deur staats-, nasionale- of internasionale entiteite gevul is. Deur die manier waarop Internetgebruikers oor die Internet dink en die herhaaldelike gebruik van dié strategieë sal dit uiteindelik ook die manier waarop die reguleringsgaping gevul word, vorm (Niemczyk, 1999:7).

Volgens Niemczyk (1999) is dit onmoontlik om die verskillende maniere waarop private individue self-regulering toepas, te bestudeer. Niemczyk fokus eerder op maniere hoe individue die Internet gebruik om hulself te beskerm.

Stellenbosch University http://scholar.sun.ac.za

- **Die self-help model** glo Niemczyk (1999) gebruik private individue wanneer hulle op 'n sekere manier reageer wat die skadelike gevolge van ander mense se aktiwiteite op die Internet elimineer of minimaliseer. Self-help aktiwiteite blyk egter om eensydig te wees, want dit is nie afhanklik van ander deelnemers om doeltreffend te wees nie.

Tegniese "regstellings", soos om 'n e-pos adres te blok, kan die meeste van die tyd die beste metode wees om mense van aanstootlike aktiwiteite te beskerm sonder om op ander staat te maak. Die self-help benadering word die beste verduidelik deur na verskillende self-help-reaksies op verskillende "waarneembare euwels" soos pornografie te kyk.

Veronderstel pornografie is 'n waarneembare euwel en dat ouers filtreringsprogramme gebruik om kinders te verhinder dat hulle aan aanstootlike materiaal blootgestel word. Die volgende is voorbeelde van sulke filtreringsprogramme wat toegang tot webwerwe verbied wat as onaanvaarbaar vir kinders beskou word.

- Net-Nanny (http://www.netnanny.com)
- Cybersitter (http://www.cybersitter.com)
- Surf Watch (http://www.surfwatch.com)

'n Ander probleem wat gereeld in huishoudings met Internet-toegang hanteer moet word, het betrekking op "spamming" oftewel ongevraagde e-pos (gewoonlik advertensies). Programme kan geskryf word wat outomaties ongevraagde e-posse skrap om die effek van "spamming" te verlig (Niemczyk, 1999:7).

Volgens Niemczyk (1999) is die tegnologiese "regstellings" wat deur self-help-metodes gebruik word nie 'n onfeilbare oplossing nie. Dit moet egter nie mense ontmoedig om van die self-help benadering gebruik te maak nie. Een Amerikaanse hof het sy mening uitgespreek oor hoe belangrik self-help metodes is. In 'n verhoor vir die voorlopige geregtelike verbod op 'n afsender van ongevraagde e-pos, het die hof in *CompuServe Inc. v. Cyber Promotions, Inc.* kennis geneem van die gebruik van self-help metodes en gevoel dié metode is veral van toepassing op sulke tipe situasies en moet toegepas word voordat regsaksie gepas is (Niemczyk, 1999:7).

- **Kollektiewe aksie** verskil van die self-help-metode deurdat dit nie net skadelike gedrag van ander verlig nie, maar omdat dit 'n verandering in ander se gedrag afdwing. Die doeltreffendheid van die kollektiewe aksie hang af van die kollektiewe magte van die deelnemers en die legitimiteit van die bedryf deur informele reëls neer te lê.

Kollektiewe aksie word gewoonlik deur middel van boikotte uitgevoer. 'n Voorbeeld van 'n kollektiewe aksie is die "Realtime Blackhole List" (RBL) wat 'n komponent van die "Mail Abuse Prevention System"-projek is. Dit is 'n inisiatief wat IDV's onder druk plaas om hul dienste en beleide so aan te pas sodat dit nie aanloklike moontlikhede vir "spammers" bied nie. As die IDV

Stellenbosch University http://scholar.sun.ac.za

nie aan die vereistes voldoen nie, sal die RBL-lede hul kollektiewe kragte gebruik om boodskappe van die IDV te blokkeer (Niemczyk, 1999:7).

- **Private kontrakte** is 'n gunsteling van Internet-ondernemings om gedrag op die Internet te reguleer. Dit is nie verbasend nie as 'n mens kyk na die toepasbaarheid van die kontrakmodel en die gemak waarmee dit vir Internet-transaksies gebruik word. Kontrakte is essensieel private wette wat betrekking het op individuele omstandighede. Die bron van hul legitimiteit lê in die gesamentlike toestemming van die betrokke partye om by die voorwaardes van die ooreenkoms te hou (Niemczyk, 1999:8).

Kontrakte op die Internet word gewoonlik gevorm wanneer gebruikers toegang tot 'n webtuiste wil hê of inhoud van daardie webtuiste wil aflaai. Voorbeelde van private kontrakte op die Internet:

- **Ticketmaster** verbied die gebruik van die webtuiste sonder dat daar ingestem word tot 'n gebruikersooreenkoms.
- **Microsoft Clip Gallery** vereis dat die gebruiker instem met sy *Addendum to the End Users Licence Agreement*.
- **PCLaw** vereis instemming tot 'n ooreenkoms voordat die gebruiker sagteware van die webtuiste kan aflaai (Niemczyk, 1999:8).

Dié tipe ooreenkomste het begin om standaard ondernemingspraktyk te word in die afwesigheid van 'n eenvormige liggaam van Internet-wetgewing.

Internetdiensverskaffers (IDV's) is al die hekwagters van die Internet genoem aangesien die meeste mense toegang tot Internet deur IDV's verkry. Regulering van die Internet kan sistematies by die "poorte" gebeur. Daarom is dit nie verbasend nie dat IDV's private kontrakte, nl. gebruiker-ooreenkomste, gebruik wat hul kliënte se gebruik van die Internet reguleer.

2.4.2 Soewereine oplossing

Die soewereine oplossing vir die regulering van die Internet bestaan uit drie benaderings:

1. Versterk nasionale regerings deur huidige regstelsels en 'n nuwe alliansie met soewereine state.
2. Skep internasionale verdrae om verskille tussen nasionale regerings op te los.
3. Stel ooreenkomste in tussen die industrie en soewereine state.

Federale nasionaliteite kan 'n bindende reguleringstelsel op verskillende maniere skep. Regulering op nasionale vlak kan byvoorbeeld baie verskillende probleme wat byvoorbeeld die VSA ervaar met die huidige wetgewing oplos. Gegewe die haakplekke van internasionale bestuur, is die VSA kongres goed geposisioneer om internasionale wette te skep wat die Internet reguleer.

Stellenbosch University http://scholar.sun.ac.za

Verdrae en "opdragte" (amptelike instruksies) tussen lande verskaf, of verskaf ten minste teoreties, 'n belans tussen lande. Dit is strukture wat nodig is om 'n stabiele Internet regstelsel te bou (Niemczyk, 1999:8).

Nasionale regerings kan buigsame regulering skep, soortgelyk aan die verdrae en opdragte met soewereiniteite, deur ooreenkomste met die nodige markleiers.

Regerings is reeds besig om ooreenkomste met Internet-koöperasies te skep. In 1998 het die VSA se Departement van Handel en ICANN (Internet Corporation for Assigned Names and Numbers) 'n memorandum van skikking verkry waar ICANN domeinname sou uitreik op so 'n manier wat die ontwikkeling van sterk mededinging sou toelaat (Niemczyk, 1999:8).

Dit blyk of die Internet nuwe, unieke uitdagings vir regstelsels inhou, maar in werklikheid is die meeste van die uitdagings nie nuut nie (Niemczyk, 1999:8).

2.4.3 Internasionale Internet-regeringsliggaam

Niemczyk (1999) glo 'n internasionale Internet-reguleringsliggaam is 'n moontlike oplossing vir die probleme van die Internet. Só 'n liggaam bied 'n stelsel van wigte en teenwigte, wat soos die Amerikaanse regeringstelsel werk, maar op 'n globale skaal.

So 'n "kuberregering" sal volgens Niemczyk (1999) uit drie aparte, maar gelyke bene bestaan: Die kuber-uitvoerende mag, die kuber-wetgewer, en die kuber-jurisdiksie. Elke been sal onafhanklik van die ander funksioneer, maar sal ook onderwerp word aan die ander se aksies.

Niemczyk (1999) bespreek ook die verskeie probleme wat self-regulering en regulering deur soewereine state na vore bring en dat die beste oplossing tog 'n vorm van internasionale kuberregering sal wees.

In A.M. Froomkin se studie "An Introduction to the 'governance' of the Internet" (1995) maak Froomkin die stelling dat die Internet 'n komplekse en meestal self-regulerende stelsel is.

> "Alhoewel nasionale regerings en 'n paar internasionale ooreenkomste sekere aspekte van die Internet reguleer, dek die regulasies 'n paar van die tegniese norme en bykans geen van die sosiale norme nie" (Froomkin, 1995:15).

Besluitneming wat betrekking het op fundamentale aspekte van Internet-bestuur word primêr deur konsensus deur verskillende Internet-organisasies bereik. Die proses van konsensus vorming neem verskeie vorme aan:

- **onderhandelingskonsensus:** eksplisiete konsensus of byna konsensus wat bereik is ná onderhandelings met alle betrokke partye

Stellenbosch University http://scholar.sun.ac.za

- **markkonsensus:** waar die *de facto* tegniese norme ontstaan deur die massa-aanvaarding van 'n spesifieke produk of 'n norm wat verhewe is bo sy mededingers
- **verbinding:** 'n vertroude party, gewoonlik 'n individu of klein komitee, word as kundig genoeg beskou om besluite te neem wat deur ander (soms outomaties) geïmplementeer word.
- **massa-wraakneming:** Internetgebruikers reageer teenoor waarneembare gevaar deur of verbanning of om elektroniese aanvalle (byvoorbeeld "e-posbomme" – ongevraagde e-pos) op diegene te doen wat nie daarin slaag om by die fundamentale sosiale norme te bly nie (Froomkin, 1995:17).

Volgens Froomkin (1995) het nasionale regerings slegs gedeeltelike beheer oor Internet-regulering, veral nadat die Internet 'n internasionale fenomeen geword het.

2.4.4 Ontwikkeling van Suid-Afrikaanse regulering

In 2001 het talle Suid-Afrikaners na die langverwagte groenskrif op Elektroniese Kommunikasie en Transaksies-wetsontwerp deur die Departement van Kommunikasie uitgesien. Die groenskrif moes openbare debat voer oor wat die beste manier sou wees om elektroniese handel in Suid-Afrika te bevorder.

Alhoewel dit 18 maande geneem het om die groenskrif te produseer, het die Departement van Kommunikasie besluit om die proses te versnel en die witskrif uit te deel. Die Parlement moet nou besluit of dié wetsontwerp voldoende is. Daar is min Suid-Afrikaanse ondernemings of verbruikers wat nie deur die Elektroniese Kommunikasie en Transaksies-wetsontwerp geraak gaan word nie (Vegter & De Wet, 2002:27).

Slegs die informeelste ondernemings wat nie 'n webwerf het nie, wat nie e-pos gebruik nie en wat geen rekords van hul kliënte op 'n elektroniese databasis het nie, kan die nuwe wetgewing ignoreer. Selfs ondernemings wat bevoordeel word deur die vinniger en goedkoper sakeprosedures wat moontlik gemaak gaan word wanneer alle vereistes vir papier-dokumentasie wegval, sal 'n prys betaal vir dié vooruitgang. Dit sal gebeur wanneer ondernemings deur die wet en nie deur mededingende druk nie, gedwing word om sekere aspekte van hul webblaaie, produksievloei en kliënteverhoudingsbestuurstelsels aan te pas. Vir verbruikers lyk die situasie beter, selfs al is die verbruikerbeskermingsklousules as swak gekritiseer. Dit word algemeen beskou as 'n verbetering van die huidige tekort/afwesigheid van beskerming (Vegter & De Wet, 2002:29-30).

Stellenbosch University http://scholar.sun.ac.za

Die Elektroniese Kommunikasie en Transaksie Wet van 2002 behels in kort die volgende:

Die Elektroniese Kommunikasie en Transaksie Wet van 2002:
'n Opsomming

- Alle e-pos, Internet en ander elektroniese boodskappe word regstatus gegee.
- Alle dokumente en verdrae wat gewoonlik deur wetgewing in skrif, onderteken, behou of in die oorspronklike formaat moes wees, kan nou in elektroniese formaat wees.
- Elektroniese dokumente kan nou as getuienis by howe ingedien word.
- Elektroniese handtekeninge word regterlike erkenning gegee en het dieselfde regstatus as ink-op-papier handtekeninge.
- Regsverdrae mag nou aanlyn en elektronies afgesluit word.
- E-pos word beskou as gestuur "wanneer dit 'n inligtingstelsel buite die beheer van die skepper betree" of "wanneer dit moontlik word vir die geadresseerde om die boodskap te bekom".
- Die stuur van 'n e-pos sal van die skepper afgestuur beskou word wanneer (1) dit deur die skepper gestuur is, (2) deur 'n persoon gestuur is wat die mag/reg gehad het om dit van die skepper af te stuur en (3) gestuur is deur die inligtingstelsel van die skepper of sy maatskappy wat deur hom geprogrammeer is.
- Erkenning van ontvangs van 'n e-pos is nie 'n vereiste vir 'n regskontrak om in werking te tree nie.
- Ooreenkomste wat met elektroniese agente, soos webwerwe, gesluit is, word regseffek gegee.
- Spesifieke brokkies inligting moet aan 'n aanlynverbruiker verskaf word deur enige onderneming wat goedere of dienste via/oor die Internet verkoop.
- Daar sal 'n "afkoel-periode" van 14 dae wees vir goedere en dienste wat oor die Internet gekoop is vir die verbruiker om die transaksie te kanselleer.
- "Spamming" (die stuur van grootmaat ongevraagde e-pos) sal onwettig wees behalwe as sekere maatreëls nagekom word.
- Aanlyn-winkels moet goedere wat aanlyn gekoop is, binne 'n sekere tydsraamwerk aflewer.
- Sekere stappe sal deur ondernemings geneem moet word om persoonlike inligting van die Internet- of e-pos-gebruikers te verkry. Dié stappe sluit in: (1) Toestemming van die data-onderwerp. (2) Verkryging van inligting moet vir regsdoeleindes nodig wees. (3) Die ontvanger moet, in skrif, die doelwit van die verkryging van die inligting uiteen sit. (4) Die ontvanger mag nie die inligting buite die omvang van die gestelde doelwit gebruik nie. (5) Die ontvanger moet vir een jaar langer as die tyd waarin die inligting gebruik is, 'n rekord hou van die inligting en die doel waarvoor dit versamel is.
- Die huidige magte van die plaaslike domeinnaam-owerheid sal deur die Regering oorgeneem word. So 'n owerheid sal 'n alternatiewe konflikresolusie aanneem om konflikte in die .za-domein te hanteer.
- "Hacking", rekenaargebaseerde uitbuiting en bedrog word misdade.

(Vegter & De Wet, 2002: 30)

2.5 Samevatting

Die Internet is net nog 'n kommunikasie-medium wat help om die "global village" in staat te stel om tot sy volle potensiaal te funksioneer. In die "global village" kan enige individu of organisasie 'n verkoper of verbruiker, 'n uitgewer of intekenaar wees met byna geen agting vir nasionale wette of grense nie. Dít bring kommersiële-, sosiale, morele, fiskale-, politieke- en regsimplikasies na vore (Opperman, 2000:4).

Die Internet se gebrek aan grense plaas 'n groot las op tradisioneel geografies gebaseerde regstelsels (Niemczyk, 1999:1). Daarom is regulering wat spesifiek vir die Internet ontwerp is

Stellenbosch University http://scholar.sun.ac.za

noodsaaklik, aangesien bykans elke aspek van die reg deur die Internet uitgedaag word en baie regsraamwerke onvoldoende is om dit te hanteer (Opperman, 2000:37). Internasionale regstoepassing is nog meer kompleks, aangesien die meeste lande se vermoë om wetgewing toe te pas op 'n oortreding, wat as 'n misdaad onder hul wetgewing beskou word, beïnvloed word deur die bepaling van die *locus delicti*, die plek van oortreding. Misdade wat in een land plaasvind, kan nou deur middel van die Internet reg oor die wêreld plaasvind (Niemczyk, 1999:3).

Die ander probleem met die huidige regulering van die Internet is dat intellektuele eiendomsregulering nasionaal gebaseerd is. Enigeen wat op die Internet publiseer, kan intellektuele eiendomsreg of enige ander regte of wette op enige plek in die wêreld oortree. Weens die aard van die Internet sal regerings daarom gedwing word om in die toekoms wetgewing te standaardiseer (De Villiers, 2000:37).

As gevolg van die wisselvallige regulering van die Internet, sou daar verwag word dat daar geen sosiale en kulturele norme vasgestel is nie. Daar is egter nie 'n totale afwesigheid van sosiale gebruike op die Internet nie – Internet-gebruikers praat gereeld van "netiket". Dit verwys na die Internet-etiket wat deur Internet-gebruikers as sekere sosiale standaarde ingestel is. Internet-gebruikers is tans besig om gedragsnorme en verwagtinge rakende Internet-verhoudings te skep wat verby eenvoudige netiket beweeg.

Die nadeel van netiket is dat dit slegs individuele gedrag voorskryf en nie konflikte oplos wat deur gebruikers wat buite die verwagte sosiale gedrag optree, geskep word nie. Verder is netiket ook nie by magte om ernstiger oortredings en verbreking van openbare standaarde soos inligtingsdiefstel en kinderpornografie te hanteer nie (Niemczyk, 1999:6).

Dit is belangrik om te besef dat die bestaan van netiket of 'n aanlyn-moraliteit nie voldoende is nie. Die Internet het steeds regulering nodig net soos gemeenskappe wette nodig het om hul sosiale waardes en kontrakte af te dwing (Niemczyk, 1999:6).

In die Internet-reguleringstudies wat in dié hoofstuk bespreek is, is die regulering wat tans vir die Internet beskikbaar is, wat uit selfregulering en die soewereine oplossing bestaan, bespreek asook Niemczyk se voorstel van 'n Internasionale Internet-regeringsliggaam uit sy studie *International Internet: A look inside* (1999).

Selfregulering vind plaas wanneer private individue strategieë soos self-help, kollektiewe aksie en private kontrakte implementeer om hul besorgdheid oor die Internet te hanteer. Internet-gebruikers sal selfs nadat voldoende regulering geïmplementeer is, voortgaan om dié metodes te gebruik (Niemczyk, 1999:9).

Volgens Niemczyk (1999) is die probleem met selfregulering die feit dat die reëls ontwikkel is toe die Internet nog jonk, en die aantal gebruikers min. Die Internet-gebruikers het ook oor die algemeen dieselfde agtergronde gehad, naamlik wetenskaplikes, navorsers of akademici. In so 'n

Stellenbosch University http://scholar.sun.ac.za

omgewing was die selfreguleringsbenadering voldoende, omdat die Internet-gemeenskap 'n klein, intellektuele groep was, en nie die groot massas wat vandag die Internet gebruik nie. Die selfreguleringsmetode kan nie met miljoene gebruikers die Internet suksesvol reguleer nie (Niemczyk, 1999:9).

Die soewereine oplossing vir regulering van die Internet versterk nasionale regerings se regulering van die Internet deur huidige regstelsels, skep internasionale verdrae om verskille tussen nasionale regerings op te los en stel ooreenkomste in tussen die industrie en die regerings (Niemczyk, 1999:10).

Regerings se reguleringsmag oor 'n individu word op jurisdiksie gebaseer. Jurisdiksie is grootliks afhanklik van ligging en teenwoordigheid. Dié stelsel werk goed vir die regulering van aktiwiteite in die nie-Internetwêreld omdat dit op 'n geografiese model van teenwoordigheid gebaseer is. Dit is ondenkbaar om 'n regering jurisdiksie oor individue toe te staan as daardie individue onwetend 'n wet van daardie regering oortree het of nooit eens bewus was van hul teenwoordigheid in daardie land nie (Niemczyk, 1999:10).

Weens die probleme wat die Internet skep om voldoende regulering moontlik te maak, glo Niemczyk (1999) 'n Internasionale Internet-reguleringsliggaam is 'n moontlike oplossing. Só 'n liggaam sal 'n stelsel van wigte en teenwigte bied, wat noodsaaklik is vir die doeltreffende regulering van 'n globale entiteit soos die Internet.

Benewens die jurisdiksie-probleme wat nasionale regerings se regulering van die Internet skep, is meer en meer lande besig om wetgewing in te stel om die Internet te reguleer. Suid-Afrika se Elektroniese Transaksies en Kommunikasies Wet 25 van 2002 het benewens geweldige reaksie uit die privaat sektor aan die einde van 2002 in werking getree (Vegter & De Wet, 2002:29-30).

Vir dié studie van Internet-regulering in Suid-Afrika is dit noodsaaklik om sekere aspekte van die Internet in die algemeen te bestudeer. In die volgende hoofstuk sal die geskiedenis en ontwikkeling van die Internet en die demografie van Internet-gebruikers bespreek word.

Stellenbosch University http://scholar.sun.ac.za

HOOFSTUK 3
ONTWIKKELING VAN DIE INTERNET

In dié hoofstuk word die geskiedenis van die Internet, van sy ontstaan tot hoe Internet-gebruikers die Internet en Wêreldwye Web vandag ken, bespreek. Die wêreldwye tendense wat betref die demografie van Internet-gebruikers word aan die einde van die hoofstuk bestudeer.

3.1 Geskiedenis van die Internet

In 1955 het Dwight D. Eisenhower, die Amerikaanse president, aangekondig dat die VSA beplan om 'n klein satelliet te lanseer wat om die aarde sou wentel. Die USSR (Rusland) het aangekondig dat hulle dieselfde wou doen. Op 4 Oktober 1957 het Rusland eerste daarin geslaag toe Spoetnik 1 gelanseer en in 'n wentelbaan om die aarde geplaas is.

In Amerika, wat op daardie tydstip 'n gevoel van kwesbaarheid ondervind het ná die ontploffing van hul kernbom dertien jaar tevore nie, het dit hewige reaksies uitgelok. Een van die eerste stappe wat die VSA geneem het, was om ARPA (Advanced Research Projects Agency) binne die Departement van Verdediging te skep. Dit is aanvanklik DARPA genoem (Defence Advanced Research Projects Agency). Die doel van dié agentskap was om die mees gevorderde tegnologie wat vir verdedigingsdoeleindes beskikbaar was, in te span en sodoende te verhinder dat die vyand hulle weer verras (Cerf, 1993:12).

ARPA het van die land se top-wetenskaplikes voltyds in diens geneem en ook genoeg geld van die regering ontvang om top-navorsers te betrek. ARPA het aanvanklik op die buitenste ruimte, ballistiese missiele en om die toets van kernbomme te monitor, gefokus. Dit was vir die agentskap belangrik om die verskillende rekenaars wat by die projekte betrokke was, op 'n manier met mekaar te verbind ter wille van onderlinge kommunikasie, verkieslik met behulp van direkte skakels tussen die betrokke rekenaars (Cerf, 1993:13-15).

In 1962 het ARPA 'n rekenaarnavorsingsprogram onder leiding van John Licklider begin. Licklider het kort tevore 'n memorandum gepubliseer oor wat hy "*Galactic Networking*" genoem het. Dit was sy visie dat rekenaars aan mekaar verbind sou word en vir almal toeganklik sou wees.

Leonard Kleinrock, wat vir ARPA gewerk het, het intussen sý idee begin ontwikkel om inligting in "pakkette" te stuur. Dié manier om inligting te stuur het twee belangrike sekuriteitsvoordele ingehou (Leiner 2000:9).

Stellenbosch University http://scholar.sun.ac.za

Eerstens het dit beteken dat daar nie slegs op een skakel in die inligtingsketting staat gemaak hoef te word nie. As een skakel of rekenaar in die netwerk buite werking is, kon die res van die pakkette met behulp van 'n ander roete by die bestemming uitkom.

Tweedens sou dit moeiliker wees om die inligting te onderskep indien dit in stukke verdeel is (Leiner 2000:11).

In 1965 is die eerste wye-area-netwerk (WAN) geskep toe rekenaars vir 'n eksperiment van twee universiteite in verskillende state aan mekaar gekoppel is. Hoewel die eksperiment getoon het dat twee rekenaars wat so ver van mekaar verwyder is, wel inligting kon uitruil, het dit ook gewys dat die telefoonlynwisselaars veels te stadig was om dit suksesvol te gebruik.

In 1967 het dit aan die lig gekom dat MIT (Massachusetts Institute of Technology), die Nasionale Fisika-laboratorium in die Verenigde Koninkryk en die RAND-Korporasie (RAND is 'n samevoeging en verkorting van die terme "research and development") almal gelyktydig aan die ontwikkeling van WAN gewerk het. Die beste idees is ingespan om die ARPANET (ARPA-netwerk) te skep (Cerf, 1993:17). Die RAND-Korporasie is 'n Amerikaanse nie-winsgewinde organisasie wat op 14 Mei 1948 gestig is. Dié navorsings- en analiseringsorganisasie help maatskappy, ondernemings en regerings met die saamstelling van beleidsraamwerke en besluitnemingsprosesse ("RAND's History", 2002:1).

Teen 1969 is die ARPANET met vier rekenaars van verskillende universiteite in Amerika in werking gestel. Een van die redes vir die sukses van die Internet was die RFC- stelsel (Request for Comments), 'n reeks notas wat vryelik onder wetenskaplikes versprei is. Dit is aanvanklik in gedrukte vorm gedoen, maar later oor die netwerk deur middel van FTP (File Transfer Protocol).

In dié notas is nuwe idees voorgestel wat die ander wetenskaplikes dan kon gebruik of verbeter. In die maande daarna het wetenskaplikes aanhou werk aan die sagteware om die netwerk te verbeter en al hoe meer rekenaars is aan die netwerk gekoppel. Teen 1971 was daar reeds 23 rekenaars aan die netwerk gekoppel.

In Oktober 1972 is ARPANET tydens die eerste Internasionale Konferensie oor Rekenaars en Kommunikasie in Washington aan die publiek bekend gestel. Dié uitstalling het verdere navorsing oor netwerke regoor die wêreld aangemoedig en nog netwerke het kort daarna ontstaan (Leiner, 2000:14).

In 1972 het ARPANET-wetenskaplikes 'n nuwe program ontwikkel wat kommunikasie - e-pos - tussen twee persone oor die netwerk moontlik gemaak het. In 1974 het hulle saam met kundiges by Stanford Universiteit 'n gemeenskaplike taal geskryf wat verskillende netwerke in staat sou stel om met mekaar te kommunikeer. Dit was bekend as 'n TCP/IP (Transmission control protocol/Internet protocol) (Cerf, 1993:19).

Stellenbosch University http://scholar.sun.ac.za

Die ontwikkeling van die TCP/IP was 'n keerpunt in die ontwikkeling van die Internet. 'n Beleid van "oop argitektuur" is aanvaar, wat verseker het dat die Internet bestaan soos ons dit vandag ken.

Hoewel die ontwikkeling van die TCP/IP in 1974 begin het en die inligting oor die ontwerp vryelik beskikbaar was, is dit eers jare later wêreldwyd aanvaar. Dit moes byvoorbeeld aangepas word om die nuwe mikrorekenaars te akkommodeer, want al die rekenaars op die netwerk was in daardie stadium hoofraamrekenaars.

Gedurende dié tydperk het netwerk-protokol en -tegnieke teen mekaar gekompeteer en was daar nie juis sprake van 'n gestandaardiseerde stelsel nie. ARPANET was steeds die ruggraat van al die netwerke, en toe dit in 1982 die TCP/IP as standaard aanvaar het, is die Internet gebore. Die Internet is 'n internasionale netwerk wat netwerke verbind wat almal die TCP/IP gebruik (Cerf, 1993:20-21).

3.1.1 Van Internet tot Wêreldwye web (www)

In 1984 het daar probleme met die Internet begin opduik omdat dit vinniger en verder gegroei het as wat ooit beplan is. Teen 1984 was daar 1 000 gasheer-rekenaars aan die Internet gekoppel en die verkeer per gasheer-rekenaar was as gevolg van die sukses van e-pos baie groot. Daar is toe voorspel dat die hele netwerk in duie sou stort vanweë die oorlading (Leiner, 2000:16).

Twee gebeure het gesorg dat die Internet oorleef het. Die eerste was die bekendstelling in 1984 van DNS (Domain Name Servers). Voor DNS het elke rekenaar sy eie naam gehad, en was daar 'n lys op die Internet beskikbaar met elke rekenaar se naam en adres wat bestaan het uit 'n reeks syfers (Cerf, 1993:23).

Die nuwe stelsel was eenvoudiger: gasheer-rekenaars se name is opgedeel in onder meer .edu (onderwys), .com (kommersieel), .gov (regering) en .org (internasionale organisasies). Verder is daar ook aan elke land 'n kode toegewys (bv. .za vir Suid-Afrika). Dié veranderinge het die name van die gasheer-rekenaars makliker gemaak om te onthou en te gebruik. Die stelsel het nou self elke naam in syfers gekodeer wat die Internet-adres van die gasheer-rekenaar of netwerk is.

Die tweede gebeurtenis was die besluit deur veral die VSA en Brittanje om die gebruik van die Internet by universiteite onder al die studente, en nie net die wetenskaprigtings nie, aan te moedig. Brittanje het JANET (Joint Academic Network) by sy universiteite begin en die VSA het die NSFnet (National Science Foundation Network) begin (Leiner, 2000:16).

Die NSFNet se vyf super-rekenaars was egter beperk tot gebruik vir navorsings- en onderrigdoeleindes. Dit het die verkeersopeenhoping laat verdwyn en gehelp om die gebruik van die Internet aan te moedig. Teen 1986 was daar 5 000 gasheer-rekenaars aan die netwerk gekoppel

Stellenbosch University http://scholar.sun.ac.za

en 'n jaar later het dié getal tot 28 000 gestyg. Die uitsluiting van kommersiële gebruikers van die netwerk het die ontwikkeling van privaat-Internet-dienslewering laat posvat (Cerf, 1993:24).

In 1987 is die eerste Internet-diensverskaffer waarvoor kliënte ledegeld betaal, UUNET, gestig en verskeie ander het gevolg. Die mense wat van Internetdiensverskaffers gebruik gemaak het, het dit hoofsaaklik vir e-pos, studiegroepe, gespreksgroepe en speletjies gebruik. Die hoofredes hiervoor was:

- Die inligting wat op die Internet beskikbaar was, was hoofsaaklik van 'n hoogs wetenskaplike aard en was slegs in teksvorm;
- Die bevele wat nodig was om inligting te verkry, was ingewikkeld;
- Dit was moeilik om inligting op die Internet op te spoor;
- Dit het baie lank geneem om inligting af te laai.

Deurslaggewende verandering in 1990 het 'n nuwe era in die ontwikkeling van die Internet ingelui. In 1990 is die oorspronklike ARPANET, wat vanaf 1983 nie meer vir militêre-navorsingsdoeleindes gebruik is nie, beëindig (Cerf, 1993:24-25).

Die eerste soek-enjin, Archie, om rekenaarlêers op die Internet op te spoor, is in 1990 by McGill Universiteit in Montreal ontwikkel. In 1991 is die beperking op die NSF se superrekenaars opgehef en kon almal van hierdie diens op die Internet gebruik maak.

Die Amerikaanse regering het ook in dié tyd die *Information Superhighway*-projek begin. Reuse-bedrae geld is vanaf 1992 tot 1996 in die VSA vir die ontwikkeling van die infrastruktuur van Internet en vir rekenaarnavorsing begroot.

Nog 'n belangrike gebeurtenis was in 1991 toe die publiek aan die Wêreldwye Web (www) bekendgestel is. Die www is 'n deel van die Internet wat gesorg het dat dit onder die breë publiek baie gewild geraak het.

Die www is 'n abstrakte inligtingsruimte. Op die Internet kry jy rekenaardata, op die www kry jy dokumente, klank, video's, enige vorm van inligting. Op die Internet is kabels die verbinding tussen rekenaars; op die www is die verbindings hiperteks-skakels (Leiner, 2000:19).

Volgens Tim Berners-Lee, een van die stigters van die www, was die droom om die Wêreldwye Web 'n algemene inligtingsentrum te maak waar almal kan kommunikeer deur inligting met mekaar te deel. Hiervoor is die www se universaliteit noodsaaklik: die feit dat 'n hiperteks-skakel na enigiets toe kan skakel (Bolmer, 2002:1-2).

Stellenbosch University http://scholar.sun.ac.za

3.2 Aan wie behoort die Internet?

Ongeveer 100 jaar gelede het 'n verbeeldingryke dief, "baron" Jay Gould, 'n wonderlike idee gehad. Hy het 'n klompie treinondernemings in St. Louis, VSA, georganiseer en saam het hulle beheer oor die twee treinbrûe in die dorpie verkry. Dié koalisie het begin om geweldige fooie vir enige teenstander te vrae wat dié brûe wou gebruik. Dit het so voortgegaan totdat die Hooggeregshof dié winsgewende speletjie gestop het in die bekende 1912 saak, *U.S. vs. Terminal Railroad Assn.* Die brûe is as noodsaaklike geriewe vir die plaaslike treinbedryf beskou en gevolglik het die hooggeregshof Gould & Co. gedwing om dit op 'n gelyke basis vir almal oop te stel (Carny, 2000:58).

Ondernemings regoor die tegnologiese landskap kry toenemend meer beheer oor kritieke dele van die Internet se infrastruktuur. Teenstanders en verbruikersgroepe kla dat monopolieë onregverdig voordeel uit hul mag neem - of is ten minste in 'n posisie om dit te doen. Reguleerders is besig om weer na sake soos die *Terminal Railroad* te kyk en vra fundamentele vrae soos: Hoeveel verantwoordelikheid het 'n monopolie om sy private eiendom met teenstanders te deel? Of, om dit anders te stel, wanneer behoort die regering 'n sleutel-tegnologiese "brug" oop te forseer? (Carny, 2000:58).

Alhoewel die debat nou eers begin, neem reguleerders reeds stappe om die beginsel van toeganklikheid in die digitale ekonomie te beskerm. In Mei 2000 het 'n Franse hof besluit dit is onwettig vir *France Télécom* om koordlose Internetverbruikers te dwing om na hul webblad te gaan. Hulle moet eerder 'n keuse tussen 'n verskeidenheid koordlose portale gebied word.

Die debat oor die toeganklikheid van die digitale ekonomie jukstaponeer filosofies twee opponerende beginsels: respekteer private eiendom en die instandhouding van die vermoë om mee te ding. Aan die een kant, sê die VSA se Federale Handelskommissie-voorsitter, Robert Pitofsky, wil mense nie stilsit terwyl ondernemings die Internet in 'n reeks monopolieë verander nie (Carny, 2000:58). "Aan die anderkant, wil hulle nie ondernemings afraai om in die Internet te investeer, deur die vrugte van hul arbeid met ander te deel nie" (Carny, 2000:58).

Sommige van die inligtingsindustrieë het 'n natuurlike neiging tot monopolieë. Hoe meer mense 'n sekere digitale produk of diens gebruik, bv. *Microsoft* se bedryfsisteem of *AOL* se kits-boodskappe ("instant messaging"), hoe aantrekliker is dit in vergelyking met opponente se produkte. Mettertyd lei dit tot monopolieë.

Dít bekommer voorstanders van toeganklikheid. Hulle glo in die eenvoudige beginsel dat inligting daartoe in staat moet wees om vrylik van die een punt van die globale kommunikasienetwerk na die ander te kan beweeg. Nog 'n regverdiging vir toeganklikheid, sê

Stellenbosch University http://scholar.sun.ac.za

voorstanders, is dat dit ontwikkeling aanmoedig. Wanneer 'n onderneming 'n sleutel-aspek van die infrastruktuur beheer, kan dit opponente se aanslae op monopolieë verhinder.

Teenstanders van toeganklikheid glo weer gedwonge toegang deur die regering kan ook die teenoorgestelde tot gevolg hê - beperk ontwikkeling en demp investering. Nog kritiek teen toeganklikheid is dat dit groot regulering tot gevolg kan hê (Carny, 2000:58).

Die Wêreldwye Web (www) is as 'n gedesentraliseerde netwerk vir die gratis uitruil van inligting en idees geskep. Waar Internet-toegang in die verlede slegs vir die intellektueles was, het dit meer en meer hoofstroom begin raak (Bolmer, 2002:2).

Volgens Noah A. Bolmer se artikel in *The Internet Law Journal*, "When Push Comes to Shove: Who Controls Where and How We surf the Web" (2002) is IDV's (Internet-diensverskaffers) die hekwagters van die inligting op die Internet. As IDV's beheer watter inligting op die www kom, watter inligting uitgestuur word en teen watter spoed, mag die Internet dalk nooit sy volle potensiaal bereik nie.

Tog beheer IDV's sy intekenare se ervaring van die Internet en www. IDV's kan intekenare verhinder om na mededingers se webwerwe te gaan of die spoed waarmee inligting van daardie webwerf afgelaai word, stadiger maak. So verhinder IDV's intekenare om te besluit waarheen hulle wil gaan en wanneer hulle soontoe wil gaan (Bolmer, 2002:2).

Die hekwagters kan ook Internet-gebruikers se vermoë om hulle eie inhoud te skep en te versprei, beperk. Die verlies van toeganklikheid sal sorg vir die verdwyning van 'n diverse en demokratiese medium en die koms van 'n medium wie se gebruikers slegs volgens die diskresie van die Internet-hekwagters kommunikeer (Stein & Kidd, 2000:1).

Tog is daar nie een spesifieke organisasie, onderneming of regering aan wie die Internet behoort nie. Inidividue en organisasies het regte tot die webwerwe wat hulle op die Internet besit, maar daar is nie eienaarskap van die Internet in sy geheel nie. Die Internet-stelsel en -protokol word uitgevoer en onderhou deur verskeie wêreld-entiteite (Hameed, 2002:1).

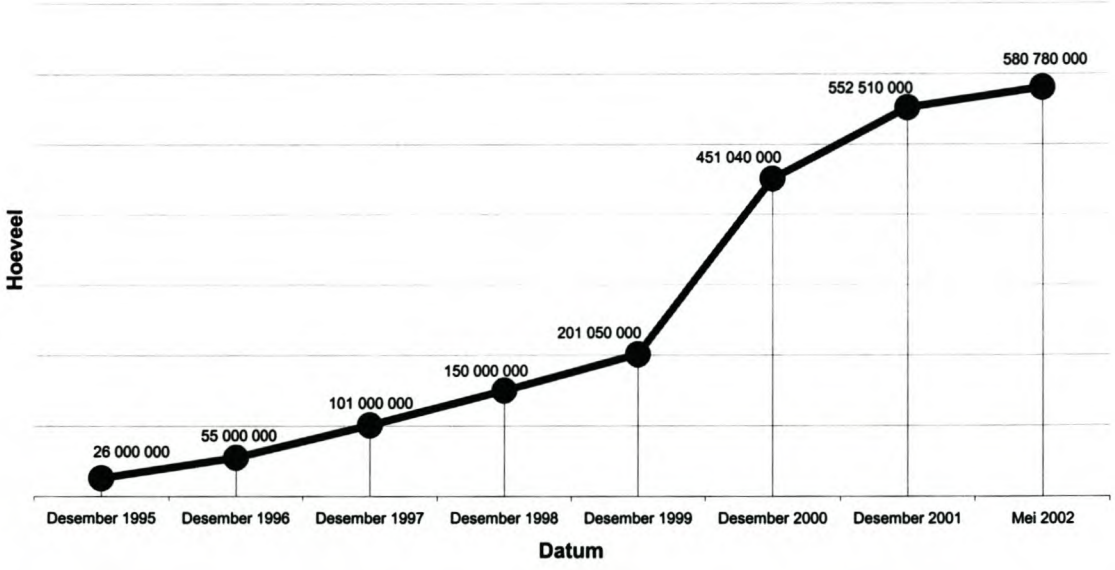
Stellenbosch University http://scholar.sun.ac.za

3.3 Demografie van Internet-gebruikers

Die demografie van Internet-gebruikers wat hier bespreek word, is slegs van toepassing op algemene tendense wêreldwyd. Die Suid-Afrikaanse demografie van Internet-gebruikers word in Hoofstuk 4 bespreek.

Sedert die begin van die Internet het die aantal mense aanlyn elke jaar met 'n positiewe groeikoers vermeerder (sien Tabel 3.1) (Moses, 1999:7).

TABEL 3.1: Aantal mense aanlyn wêreldwyd: 1995 - 2002



Bron: www.nua.ie

Dit is egter belangrik om te weet wie die Internet-gebruikers is. In die afdeling sal daar 'n uiteensetting van www.survey.net se Internet-gebruikersondersoek van 1999 wees asook 'n kort bespreking van NetWatch-opname van ACNielsen. Ongeveer 6 754 Internet-gebruikers het in Maart 1999 vrywilliglik aan www.survey.net se Internet-gebruikersondersoek deelgeneem ("Internet User Survey #2", 1999:1).

ACNielsen se NetWatch is 'n internasionale opname van die Internet-gemeenskap oor die hoofstreke van die wêreld. Die NetWatch-opname strek oor 16 lande en die opnames bestaan uit 149 000 individue wat via die Internet aan die opnames deelgeneem het ("An International Survey", 2002:1).

Stellenbosch University http://scholar.sun.ac.za

NetWatch het gevind dat oor 'n groot gedeelte van die wêreld minder vroue die Internet gebruik. Volgens die opname bestaan die Internet-gebruikers byvoorbeeld in Amerika uit 30% mans en 21% vroue, in Australië is dit 29% mans en 21% vroue, in Kanada bestaan die Internet-gebruikers uit 41% mans en 34% vroue en in Singapoer is dit 41% mans en 34% vroue. Die Internet word tans as 'n oorheersend manlike domein gesien. 'n Ander duidelike tendens wêreldwyd is dat Internet-gebruikers meestal bestuursposisies beklee by hul werk. Dit is veral die tendens in lande waar die Internet mark-penetrasie nie goed is nie. Studente vorm ook 'n groot deel van die Internet-gebruikers wat volgens NetWatch dui op die onmiskenbare waarheid dat die Internet wel die kommunikasiemedium van die toekoms is ("Who is not using the Internet?", 2002:1).

Die meeste Internet-gebruikers kry toegang tot die Internet van hul huise af. Die tendens in Kanada en Nieu-Seeland wys dat Internet-toegang van die huis af sterk aan die toeneem is. Volgens NetWatch was dit slegs Indonesiërs wat 'n hoër toegang tot die Internet van die werk af het, omdat die meeste Indonesiërs dit nie kan bekostig om self 'n rekenaar te besit nie. In die Filippyne gebruik die meeste Internet-gebruikers Internet-kafee's om toegang tot die Internet te kry ("Internet Access: At Home or At Work?", 2002:1).

E-pos bly die nommer een rede hoekom mense die Internet gebruik (Sien Tabel 3.2). Dit was slegs die Filippyne waar e-pos nie bo-aan die ranglys was nie.

TABEL 3.2: Gebruike van die Internet: Top 5-ranglys van geselekteerde lande

Gebruike	Singapoer	Hong Kong	China*	Filippyne	Nieu-Seeland	Australië	VSA	Kanada
E-pos	1	1	1	2	1	1	1	1
Navorsing	4	2			4	3	3	
Aflaai van sagteware/lêers	3	5	3	5		4	4	4
Rondrits ("surfing")	2	4	2	4	2	2	2	3

Waar daar geen rang verskyn nie, was daardie Internet-gebruik nie onder die top 5 gebruike van daardie land nie.
** China - slegs 3 kern stede was deel van die opname*

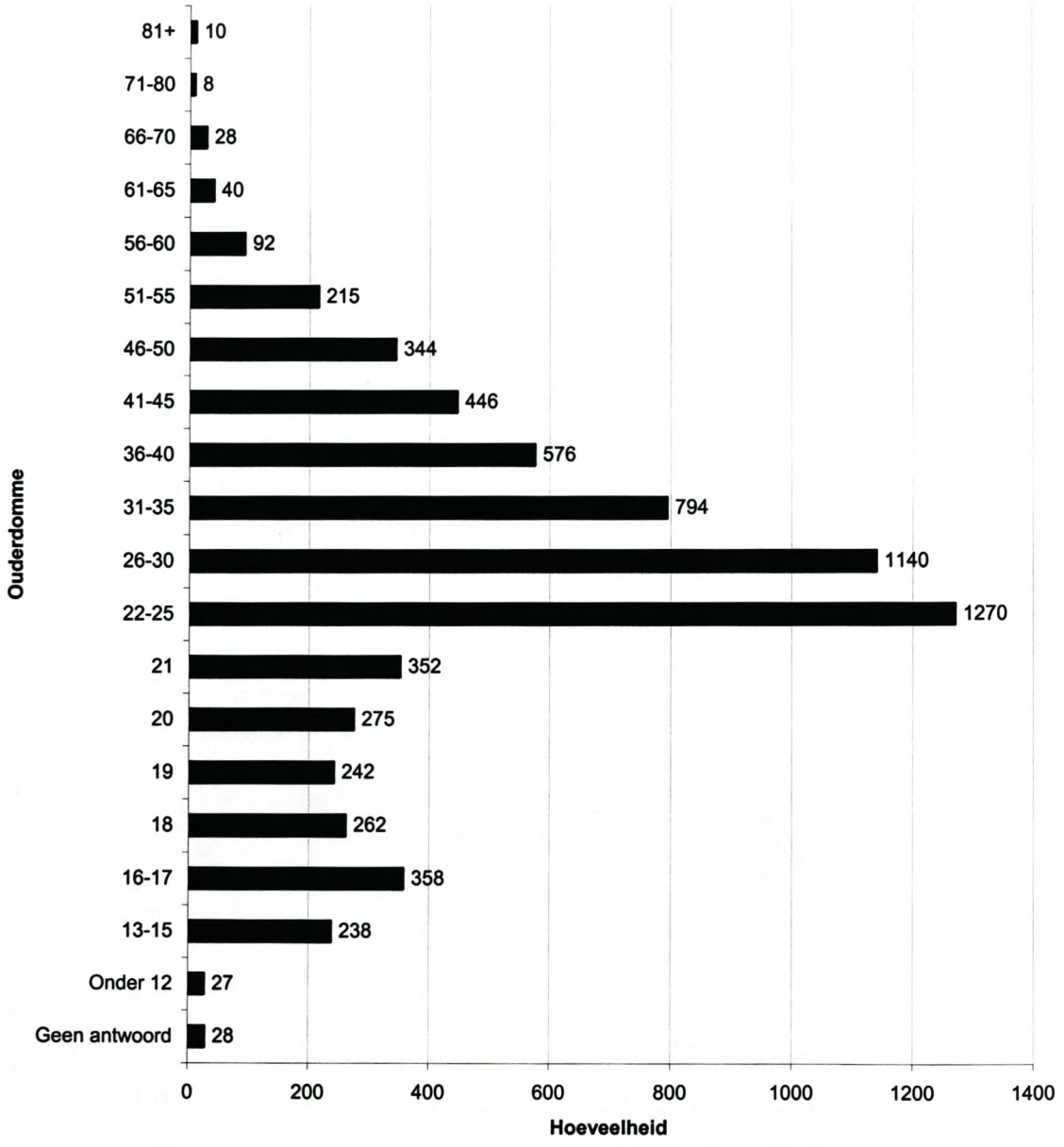
1 - nommer 1 gebruik	2 - nommer 2 gebruik	3 - nommer 3 gebruik	4 - nommer 4 gebruik	5 - nommer 5 gebruik

Bron: www.acnielsen.com

Stellenbosch University http://scholar.sun.ac.za

Volgens www.survey.net se opname van 1999 is die meeste Internet-gebruikers tussen 22 en 35 jaar oud, met die meeste gebruikers wat tussen die 22-25 jaar ouderdomsgroep val (Sien Tabel 3.3).

TABEL 3.3: Ouderdom (Maart 1999)

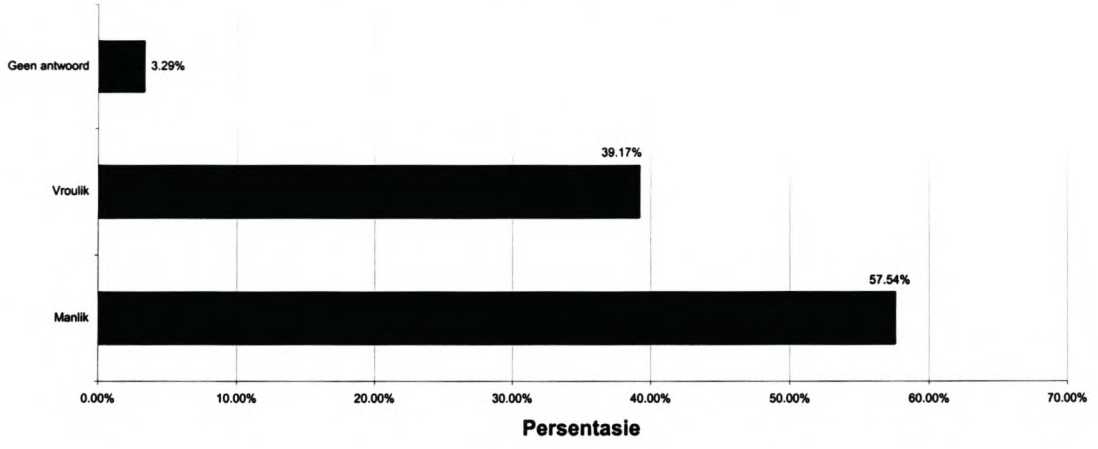


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Soos reeds uit ACNielsen se NetWatch-opname aangedui is, vorm vroue die minderheid van Internet-gebruikers. Ook www.survey.net se opname van 1999 het die tendens getoon (Sien tabel 3.4). Volgens dié opname vorm mans 57,54% van die Internet-gebruikers wêreldwyd en vroue slegs 39,17%.

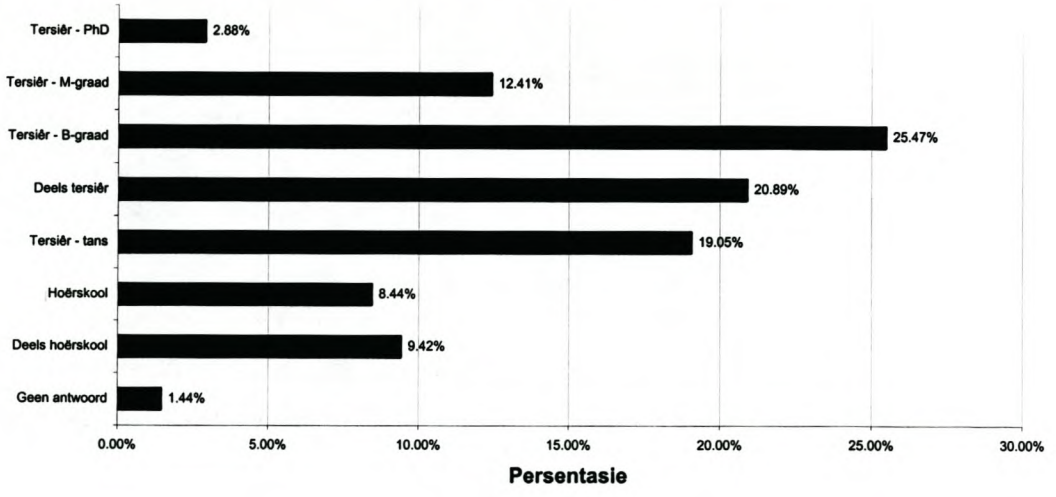
TABEL 3.4: Geslag (Maart 1999)



Bron: www.survey.net

Uit Tabel 3.5 is dit duidelik dat dit meestal mense met 'n redelike hoë vlak van opvoeding is wat die Internet gebruik. Dit is te verstane aangesien die Internet vroeër primêr deur wetenskaplikes en akademici gebruik is.

TABEL 3.5: Vlak van opvoeding voltooi (Maart 1999)

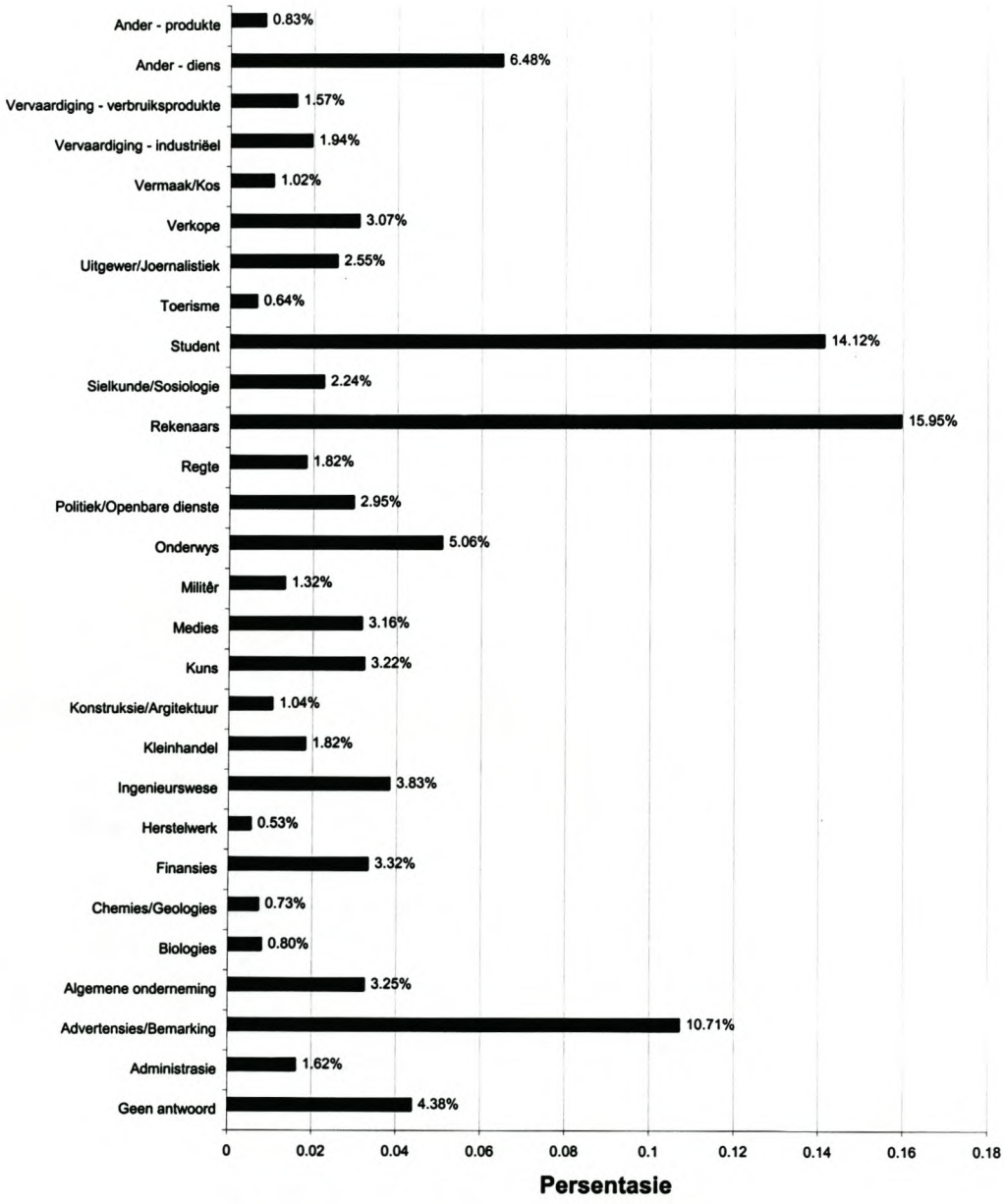


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Die meeste Internet-gebruikers is afkomstig van die rekenaarbedryf of is studente wat die Internet vir akademiese of kommunikasie-doeleindes gebruik (Sien Tabel 3.6). Die redelike hoë aantal Internet-gebruikers wat in die advertensie- of bemarkingsbedryf is (10,71%), dui daarop dat ondernemings besef hulle moet ook op dié nuwe medium hul produkte bemark/adverteer om hul teenwoordigheid in die mark te verbeter.

TABEL 3.6: Tipe werk (Maart 1999)



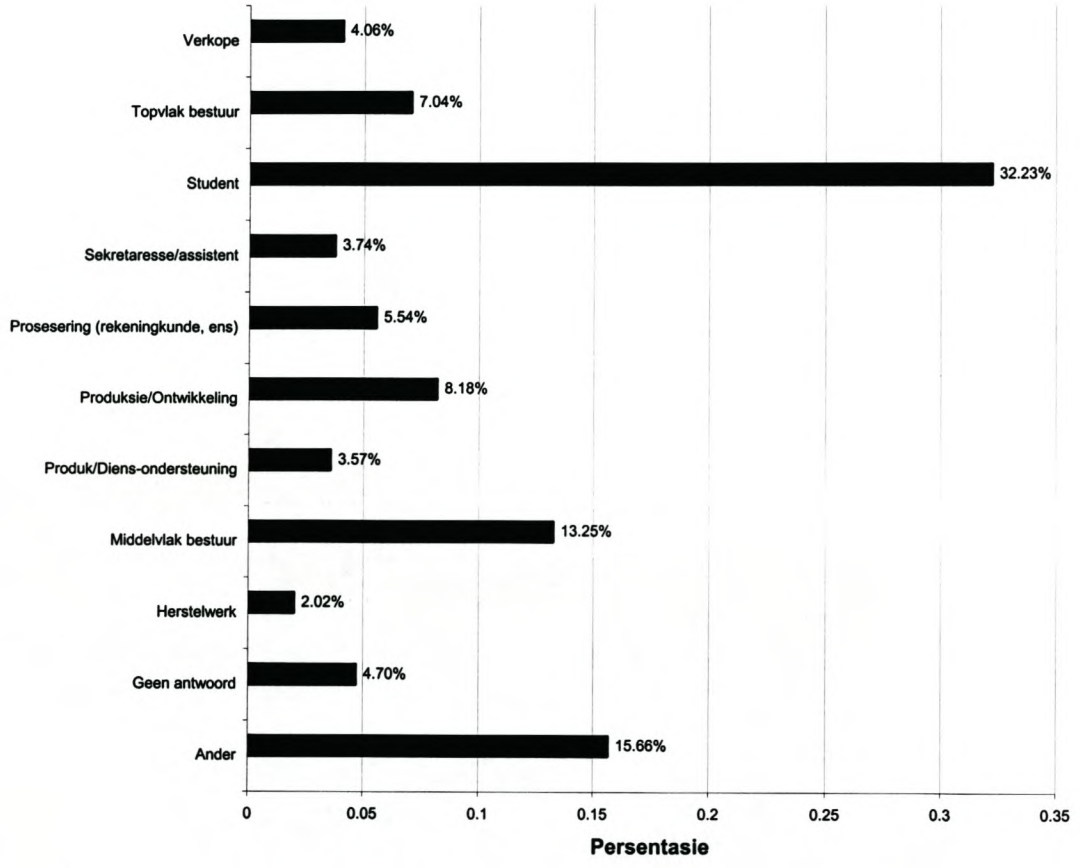
Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Volgens dié gebruikersopname van www.survey.net bestaan die meeste Internet-gebruikers uit studente (32,23%), terwyl diegene in hoë bestuursposisies slegs 7,04% van die gebruikers verteenwoordig (Sien Tabel 3.7). As 'n mens egter die topvlak- en middelvlak-bestuursposisies bymekaar tel, verteenwoordig hulle 'n meer realistiese deel (20,29%) van die Internet-gebruikers.

Volgens ACNielson se NetWatch-opname van 2001 beklee Internet-gebruikers meestal bestuursposisies. Dié verbetering in Internet-gebruik onder bestuurders dui op die noodsaaklikheid van die Internet in die werkplek en as kommunikasie-medium.

TABEL 3.7: Watter posisie beklee (Maart 1999)

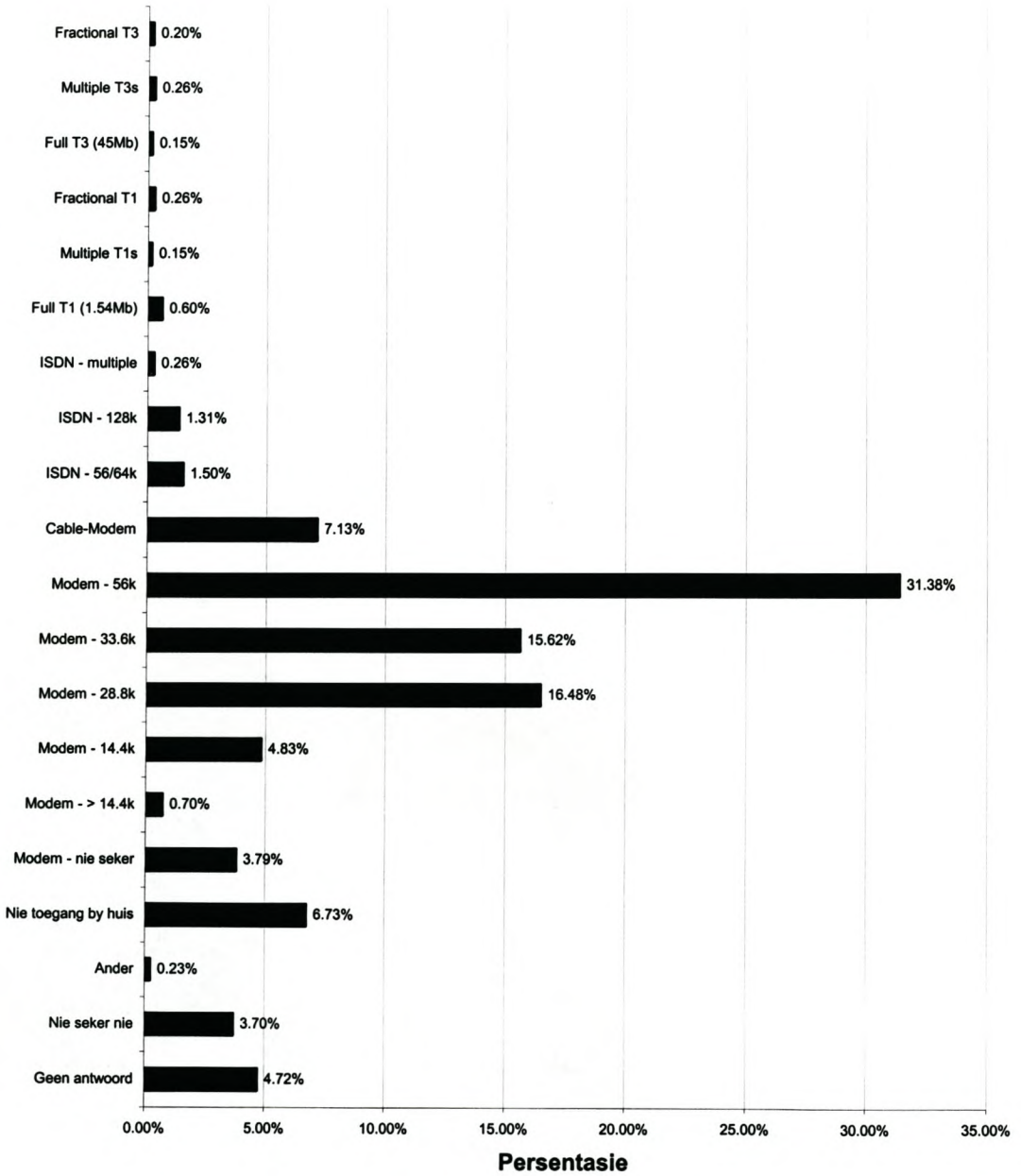


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Uit Tabel 3.8 is dit baie duidelik dat die meeste Internet-gebruikers wat die Internet van hul huis af gebruik, modems gebruik. Die spoed waarmee webwerwe van die Internet op die gebruiker se rekenaar afgelaai word, is ook belangrik aangesien 31,38% van die gebruikers 'n 56k Modem gebruik, sodat dit moontlik is.

TABEL 3.8: Maksimum spoed - huis (Maart 1999)

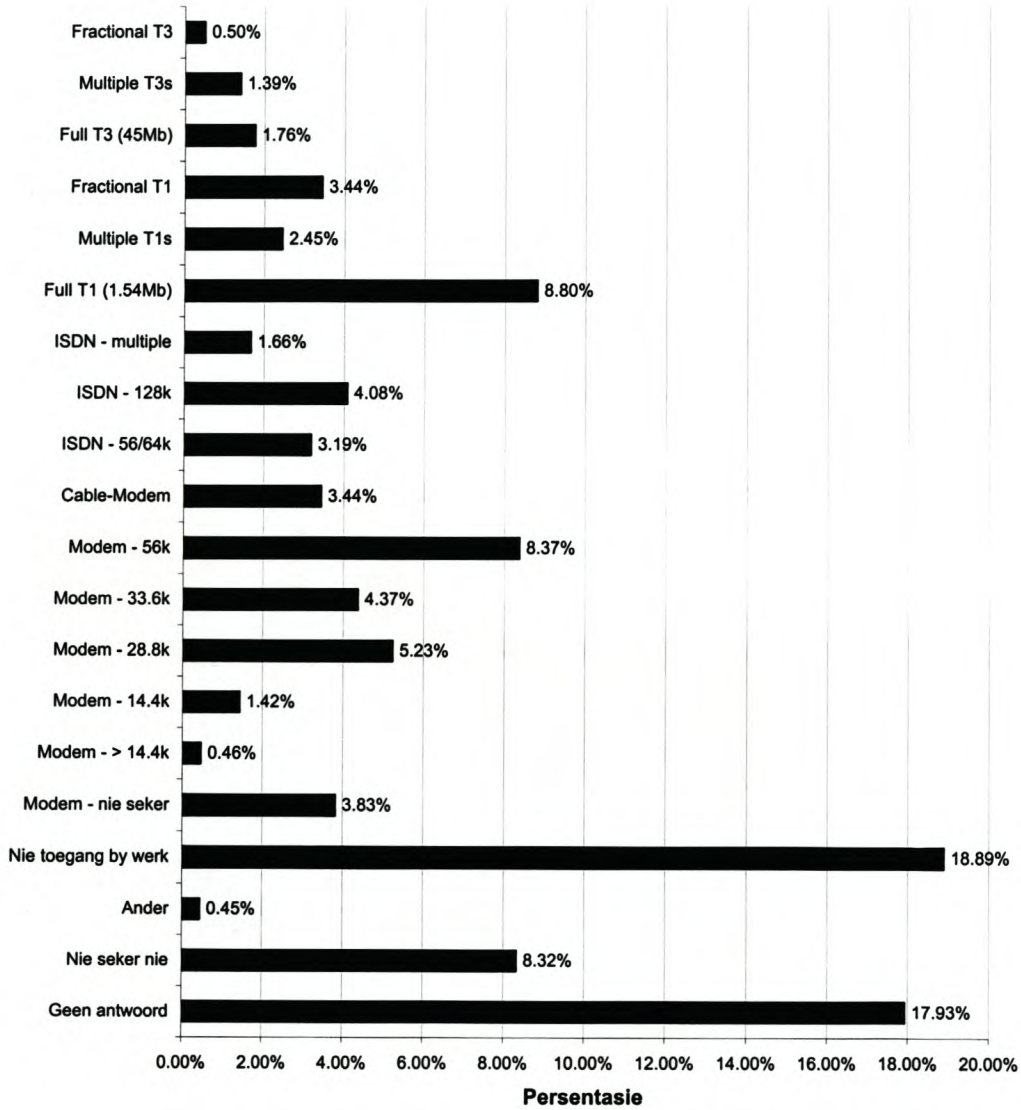


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

'n Groot gedeelte van die Internet-gebruikers weet nie watter tipe verbinding hulle by die werk tot die Internet het nie. In Tabel 3.9 het die meeste gebruikers aangedui hulle is nie seker watter tipe verbinding daar by die werk is nie of hulle het nie die vraag beantwoord nie. Dis interessant om op te merk dat 18,89% van die Internet-gebruikers wat aan www.survey.net se opname deelgeneem het, glad nie Internet-toegang by die werk het nie. Internet-toegang deur middel van 'n ISDN of modem word deur telefoonkabels moontlik gemaak. Die res word via satelliet-verbindings verskaf.

TABEL 3.9: Maksimum spoed - werk (Maart 1999)

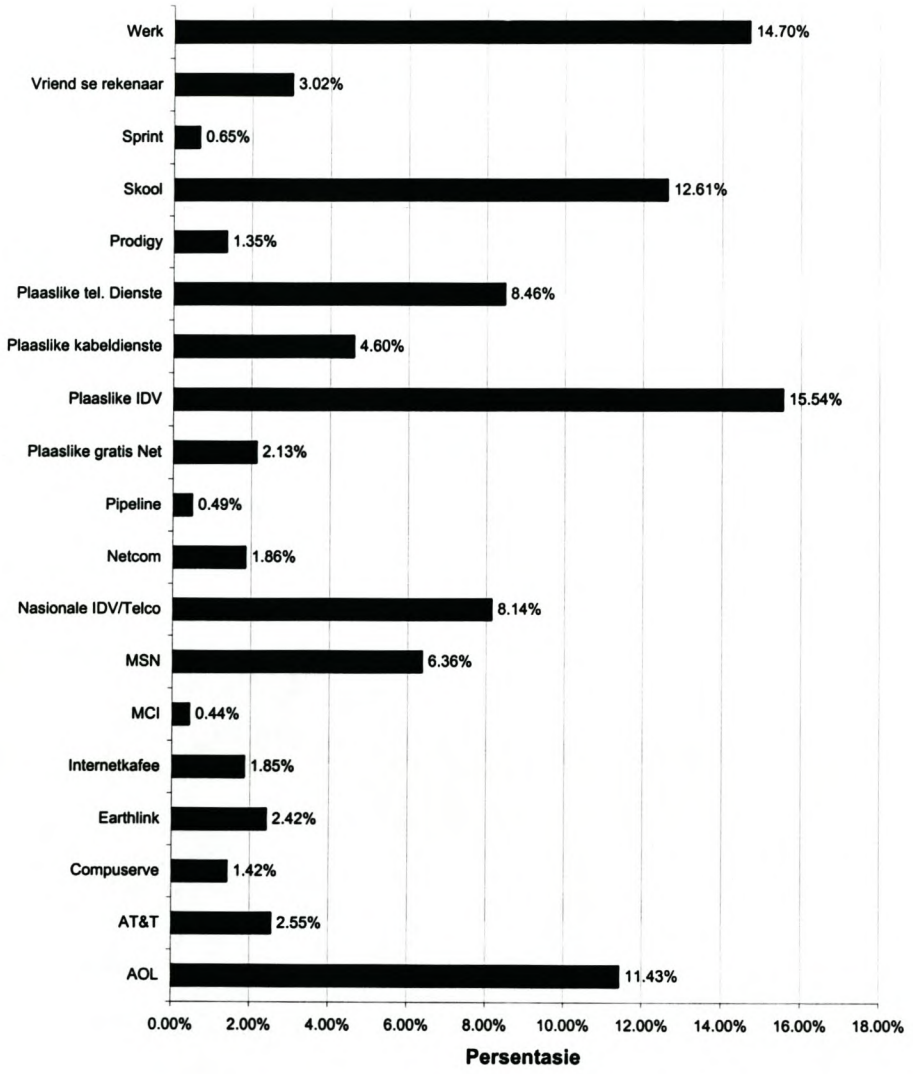


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Die meeste Internet-gebruikers kry toegang tot die Internet van hul werk af (14,7%) of deur 'n plaaslike Internet-diensverskaffer (15,54%). Volgens Tabel 3.10 is daar ook gebruikers wat toegang tot die Internet van hul skool af kry. America Online (AOL) is met 11,43% die IDV wat die beste verteenwoordig is in Tabel 3.10.

TABEL 3.10: Toegang tot Internet (Maart 1999)

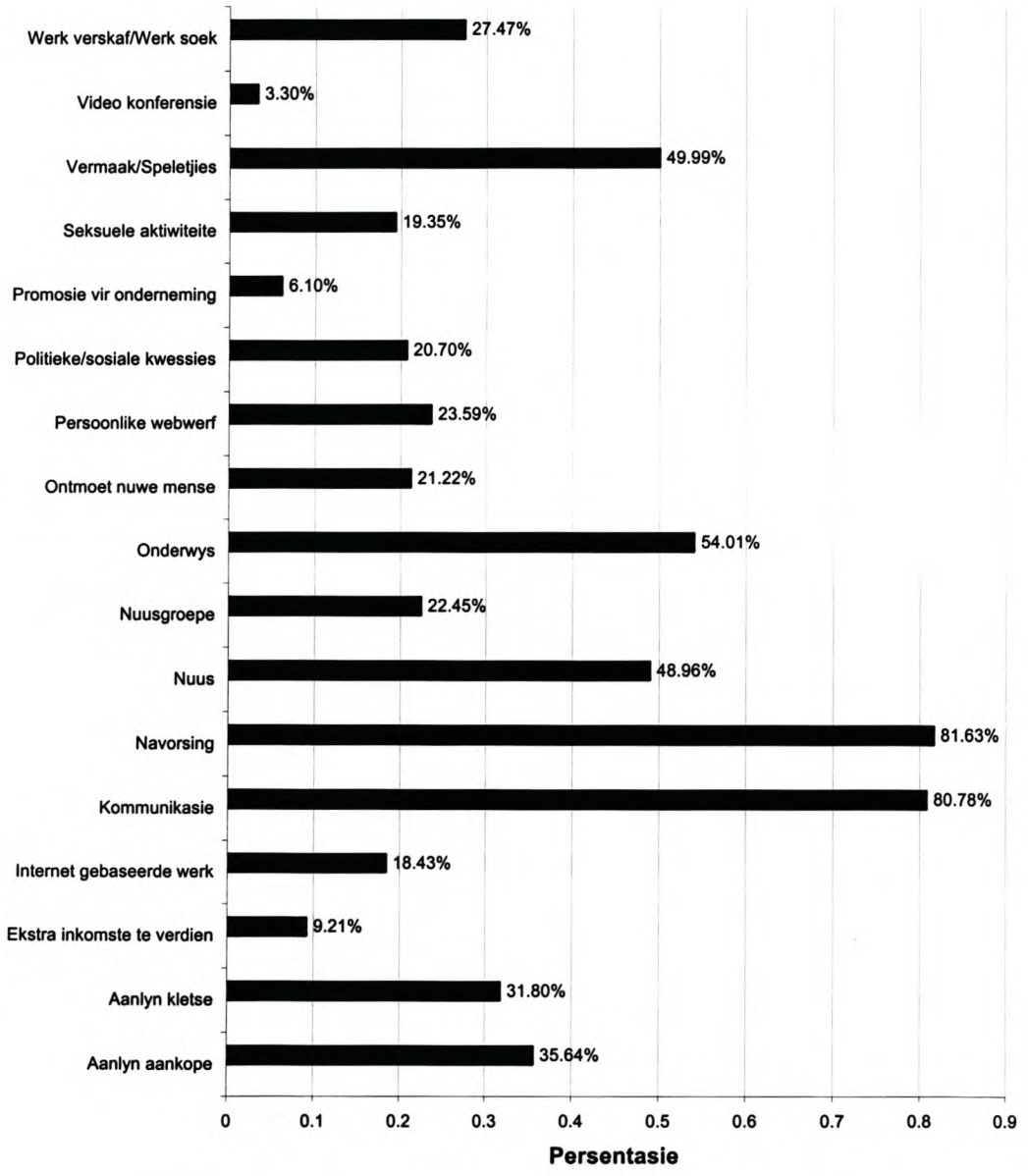


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Uit Tabel 3.11 word dit duidelik dat die Internet die kommunikasie-medium vir die toekoms is. Van die Internet-gebruikers wat aan www.survey.net se opname deelgeneem het, het 80,78% aangedui die primêre doel van hul Internet-gebruik is vir kommunikasie. Dit stem ooreen met ACNielsen se Top 5-ranglys van gebruike van die Internet soos in Tabel 3.2 aangedui. Navorsing as primêre doel vir die gebruik van die Internet is met 81,63% bo-aan dié lys. Dit is te verstane aangesien die meeste gebruikers in die opname in Tabel 3.7 aangedui het dat hulle steeds studente is.

TABEL 3.11: Primêre doel van Internet (Maart 1999)



Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

3.4 Samevatting

Die Internet het ontstaan uit die Amerikaanse Departement van Verdediging se skepping van ARPA (Advanced Research Projects Agency). Dit was vir die agentskap belangrik om die verskillende rekenaars wat by die projek betrokke was ter wille van onderlinge kommunikasie met mekaar te verbind (Cerf, 1993:12).

In 1974 is die gemeenskaplike taal wat bekendstaan as die TCP/IP (Transmission control protocol/Internet protocol) geskryf, wat verskillende netwerke in staat stel om met mekaar te kommunikeer (Cerf, 1993:16). Hoewel die ontwikkeling van die TCP/IP in 1974 begin het en die inligting oor die onderwerp vryelik beskikbaar was, is dit eers jare later wêreldwyd aanvaar. Gedurende dié tydperk het netwerk-protokol en -tegnieke teen mekaar gekompeteer en was daar nie juis sprake van 'n gestandaardiseerde stelsel nie. Toe TCP/IP in 1982 as standaard aanvaar is, is die Internet gebore (Cerf, 1993:19).

Teen 1984 het die Internet vinniger en verder gegroei as wat ooit beplan is. Twee gebeure het gesorg vir die oorlewing van die Internet:

1. die bekendstelling in 1984 van DNS, die Internet se domeinnaam-stelsel.
2. die besluit deur veral die VSA en Brittanje om die gebruik van die Internet by universiteite aan te moedig om sodoende die verkeersopeenhoping te laat verdwyn.

Nog 'n belangrike gebeurtenis was toe die publiek in 1991 aan die Wêreldwye Web (www) bekendgestel is. Die www is 'n abstrakte inligtingsruim wat die Internet onder die breë publiek baie gewild gemaak het (Leiner, 2000:19).

Daar is egter nie een spesifieke organisasie, onderneming of regering aan wie die Internet behoort nie. Individue en organisasies het regte tot die webwerwe wat hulle op die Internet besit, maar daar is nie eienaarskap van die Internet in sy geheel nie (Hameed, 2002:1).

In die volgende hoofstuk word die geskiedenis en ontwikkeling van die Internet in Suid-Afrika en die demografie van die Internet-gebruikers van die land bespreek.

Stellenbosch University http://scholar.sun.ac.za

HOOFSTUK 4
DIE INTERNET IN SUID-AFRIKA

Vir sommige mense is die Internet in Suid-Afrika 'n relatiewe nuwe fenomeen, vir ander het dit 'n lang en soms moeilike geskiedenis. In dié hoofstuk sal die geskiedenis en ontwikkeling van die Internet in Suid-Afrika bespreek word. 'n Tydlyn van die belangrikste gebeure wat betrekking het op die geskiedenis en ontwikkeling van die Internet in Suid-Afrika vorm die middelste gedeelte van die hoofstuk. Die hoofstuk word afgesluit met 'n bespreking van die demografie van die Suid-Afrikaanse Internet-gebruikers vanaf 1997.

4.1 Geskiedenis en ontwikkeling

Die Internet in Suid-Afrika het in 1988 begin toe daar 'n volhoubare e-posskakel[3] tussen die Rhodes Universiteit, Grahamstad en 'n huis in Portland, Oregon in die VSA vasgestel is. Dié skakel is later met die Internet verbind.

Dit was ongeveer dieselfde tyd wat die Uninet-netwerk (die Suid-Afrikaanse universiteite se netwerk) deur die Stigting vir Navorsing en Ontwikkeling (Foundation for Research and Development) begin is (Lawrie, 1997:1). Ongeveer teen 1986, voor die Uninet-netwerk, was daar twee netwerke tussen Suid-Afrikaanse universiteite: een tussen Rhodes Universiteit, Universiteit van Kaapstad en Universiteit van Natal in die suide en 'n ander netwerk tussen Potchefstroom Universiteit, Universiteit van Witwatersrand en die Universiteit van Pretoria en die WNNR in die noorde. Ander universiteite het later as gevolg van Uninet bygekom (Buys, 2001:35) en die twee netwerke is aanmekaar geskakel (Lawrie, 1997:2).

Die ontwikkeling van die Internet in Suid-Afrika, veral by die "liberale" Rhodes Universiteit, het tydens 'n moeilike tyd in die Suid-Afrikaanse geskiedenis plaasgevind (Lawrie, 1997:4). Weens die politieke situasie in Suid-Afrika in 1989 is toegang tot die wêreldwye Internet verbied (Buys, 2001: 35). Die apartheid-regering het onder geweldige druk van 'n groot gedeelte van die Suid-Afrikaanse bevolking gekom en het sy bes probeer om die vloei van inligting uit Suid-Afrika te beheer. Die VSA-regering se sanksies teen Suid-Afrika is dan nog nie eens in aanmerking geneem nie (Lawrie, 1997:5).

---

[3] 'n E-posskakel wat sonder enige foutiewe elektroniese opstelling e-pos tussen die twee geskakelde punte stuur.

Stellenbosch University http://scholar.sun.ac.za

Mike Lawrie, wat van die begin af betrokke was by die ontwikkeling van die Internet in Suid-Afrika en direkteur was van rekenaardienste aan Rhodes Universiteit het op 8 November 1990 'n e-pos aan Vinton G. Cerf, voorsitter van die Internet Aktiwiteite Raad (1990) in die VSA gestuur. In die e-pos vra Lawrie vir Cerf of dit moontlik is om die .za domeinnaam van Suid-Afrika met die Internet te koppel en onder die adminstrasie van die Uninet-za Beheerraad te plaas.

Cerf het 'n paar dae later vir Lawrie 'n e-pos gestuur waarin hy sê die Internet Aktiwiteite Raad het in samewerking met die Federale Netwerkraad besluit om Suid-Afrika toegang tot die Internet te gee en die .za domeinnaam te registreer. Die enigste voorwaarde is dat die verbinding tot die Internet via 'n derde party moes geskied aangesien die Amerikaanse beleid 'n direkte verbinding verbied het. Op daardie stadium was Suid-Afrika reeds deur middel van indirekte verbindings tot die Internet geskakel. Cerf het aan Lawrie voorgestel dat skakel deur 'n derde-party of 'n Europese-netwerk binne die Amerikaanse beleid toelaatbaar is (Lawrie, 1990:1).

4.1.1 Suid-Afrikaanse Internet Tydlyn

Hier volg 'n kort tydlyn (soos aangehaal in Buys, 2001:1-8) van die belangrikste gebeure wat tot die geskiedenis en ontwikkeling van die Internet in Suid-Afrika bygedra het.

1965 November	Rhodes Universiteit is die eerste universiteit in Suid-Afrika om 'n rekenaar (ICT 1301) te installeer.
	http://apies.frd.ac.za/uninet/history/
1988	Die eerste e-posskakel met die Internet word by Rhodes Universiteit ingestel.
1990	Die Suid-Afrikaanse za-domein word by die Internet Aktiwiteite Raad geregistreer en onder die administrasie van die Uninet-za Beheerraad geplaas.
	http://apies.frd.ac.za/uninet/history/
1991	Die Poskantoor Wysigingswet 85 van 1991 (Post Office Amendment Act 85 of 1991) maak voorsiening vir die stigting en vereniging van Telkom SA Beperk en die Suid-Afrikaanse Poskantoor Beperk.
1992	Die Intersepsie en Moniterings Afskaffingswet (Interception and Monitoring Prohibition Act) verbied die onderskepping van sekere kommunikasies, maar maak voorsiening vir die onderskepping van pos-artikels en kommunikasies en vir die monitering van gesprekke in geval van ernstige oortreding of indien die sekuriteit van die staat bedreig word.
	http://www.polity.org.za/govdocs/legislation/doclaw.html
1996 Junie	Uniform stel 'n eweknie-punt (peering point) met gratis toegang in vir enigiemand wat toegang tot die Internet wil hê. Aan die begin het die eweknie-punt IDV's sonder hul eie internasionele skakels, se ondersteuning gehad, maar later met die begin van ISPA (Internet Service Providers Association) se eweknie-punte en die politieke spanning tussen ISPA en Telkom het die eweknie-punt nie verder ontwikkel nie.
	http://www.internet.org.za/industry/peering.htm

Stellenbosch University http://scholar.sun.ac.za

	ISPA word gestig in antwoord teen Telkom se vorming van SAIX (South African Internet Exchange) en Intekom. Die stigterslede sluit in: Internet Solution, UUNet Internet Africa, Network Information Services, PIX, Global Internet Access en LeClub Internet Access.
	http://www.ispa.org.za
1997 Julie	ISPA is gestig in reaksie teen die waarneembare bedreiging teen die onafhanklikheid van Internet-toegang wat deur Telkom se toetrede tot die Internet-toegangsmark meegebring is. ISPA het 'n saak teen Telkom by die Kompetisie Raad aanhangig gemaak. Die Mededingingsraad (Competition Board) maak 'n tussentydse reëling oor die dispute tussen ISPA en Telkom en bevestig dat ISPA se besorgdhede aanneemlik is.
	http://www.ispa.org.za/interim_ruling.html
Augustus	Volgens ISPA het Telkom besluit om nie enige nuwe internasionale bandwydte (bandwith) aan ISPA en sy lede te verskaf nie.
	http://www.ispa.org.za/press9.html
	Die "Blou Skrif" word gepubliseer om insette aan SATRA (South African Telecommunications Regulatory Authority) en die regering oor die regulering van die Internet te lewer.
	http://www.internet.org/bluepaper.html
Oktober	SATRA maak die bevinding dat toegang tot die Internet deur VANS (Value Added Network Services) lisensie verskaf sal word en dat Telkom geen aanspraak op eksklusiwiteit het met betrekking tot die voorsiening van Internet-toegang nie. SATRA bevind ook dat 'n neutrale, industrie-geadministreerde eweknie-punt tot stand gebring moet word. Media Africa publiseer sy Internet-diensverskaffers-opname.
	http://www.mediaafrica.co.za/isp97.html
November	SATRA vra voorleggings oor die regulering en lisensiëring van VANS en Private Telekommunikasie Netwerke (PTN).
	http://www.ispa.org/submission3.html
1998 Januarie	Opheffing van ISPA se eweknie-beperkinge op Telkom en Intekom deur aan hulle toelating tot lidmaatskap van ISPA te gee.
	http://www.ispa.org.za/press14.html
Junie	ISOC SA word deur die Internet Organisasie (ISOC) goedgekeur as die amptelike liggaam van die Internet Organisasie in Suid-Afrika. Media Africa stel syfers van sy Web-handelsopname en Web-gebruikersopname vry.
	http://www.mediaafrica.co.za/webusers.html **http://www.mediaafrica.co.za/webcommerce.html**
Oktober	Die Suid-Afrikaanse liggaam van die Internet Organisasie word amptelik gestig.
	http://www.isoc.org.za/
1999 Februarie	ISOC SA verkies lede van die naamspasie-opstellingskomitee en begin om 'n naamspasie-beleid vir die top-vlak .za-domein op te stel.
	http://www.isoc.org.za/namespace.html

Stellenbosch University http://scholar.sun.ac.za

April	Die NNS (Nasionale Navorsingstigting) word ingestel deur die Nasionale Navorsingstigting Wet 23 van 1998. Die NNS bestuur die Uninet-netwerk.
	http://www.frd.ac.za
	Die Film en Publikasie Wet (Films and Publication Act) word gewysig om spesifiek voorsiening te maak vir materiaal wat deur die Internet verkry is.
	http://www.polity.org.za/govdocs/legislation/1999/index.html
2001	Die groenskrif op Elektroniese Kommunikasie en Transaksie-wetsontwerp (Electronic Communications and Transactions Bill, ECT Bill) word deur die Departement van Kommunikasie vrygestel vir openbare debat.
2002	Die Departement van Kommunikasie besluit om die proses te versnel en die witskrif op Elektroniese Kommunikasie en Transaksie-wetsontwerp word uitgedeel.
	http://brainstorm.itweb.co.za
	Die Wet op Elektroniese Kommunikasie en Transaksies tree in werking.
	http://www.polity.org.za
	'n Paneel word deur die Minister van Kommunikasie, Dr. Ivy Matsepe-Casaburri, saamgestel vir die benoeming van 'n kortlys kenners vir die za-Domein-naamowerheid. Die nege lede van die owerheid moet volgens die Wet op Elektroniese Kommunikasie en Transaksies uit verteenwoordigers van 'n wye verskeidenheid sektore saamgestel word. Lede van die publiek word kans gegee om aansoek te doen vir die owerheid deur hul CV aan zaPanel@selection.co.za te stuur. Die za internet domein-naam wat voorheen onder die beheer van mnr. Mike Lawrie was, sal deur 'n "paneel kenners" uitgereik en bestuur word (Kok, 2002:S7).
	http://www.polity.org.za
Desember	Die Wet op die Beheer van die Onderskepping van Kommunikasie word deur die parlement goedgekeur. Die verskaffers van Internetdienste in Suid-Afrika sal nou voortaan onder meer verplig word om alle e-posboodskappe van hul kliënte vir minstens drie jaar te berg.
	(De Bruin, 2003: S11)

4.2 Demografie van Suid-Afrikaanse Internet-gebruikers

In 1997 het South Africa Online (http://www.southafrica.co.za), in samewerking met The House of SYNERGY (http://www.thos.co.za), die eerste Suid-Afrikaanse Internet-gebruikersopname gedoen. Die opname is aanlyn via die Internet by http://www.southafrica.co.za/survey gedoen waar deelnemers die webwerf besoek het en 'n vraelys ingevul het. Die opname was vir 'n periode van twee maande beskikbaar en 700 mense het daaraan deelgeneem. Ander Suid-Afrikaanse Internet-gebruikers opnames wat in 1998, 1999 en 2000 gedoen is, sal kortliks bespreek word.

Volgens die opname in 1997 is die tipiese Suid-Afrikaanse Internet-gebruiker 'n getroude man, tussen 26 en 30 jaar oud en Engelssprekend. Hy is goed opgevoed (het hoërskool klaargemaak en is moontlik 'n universiteit gegradueerde) en verdien tussen R10 000 en R19 000 per maand. Hy

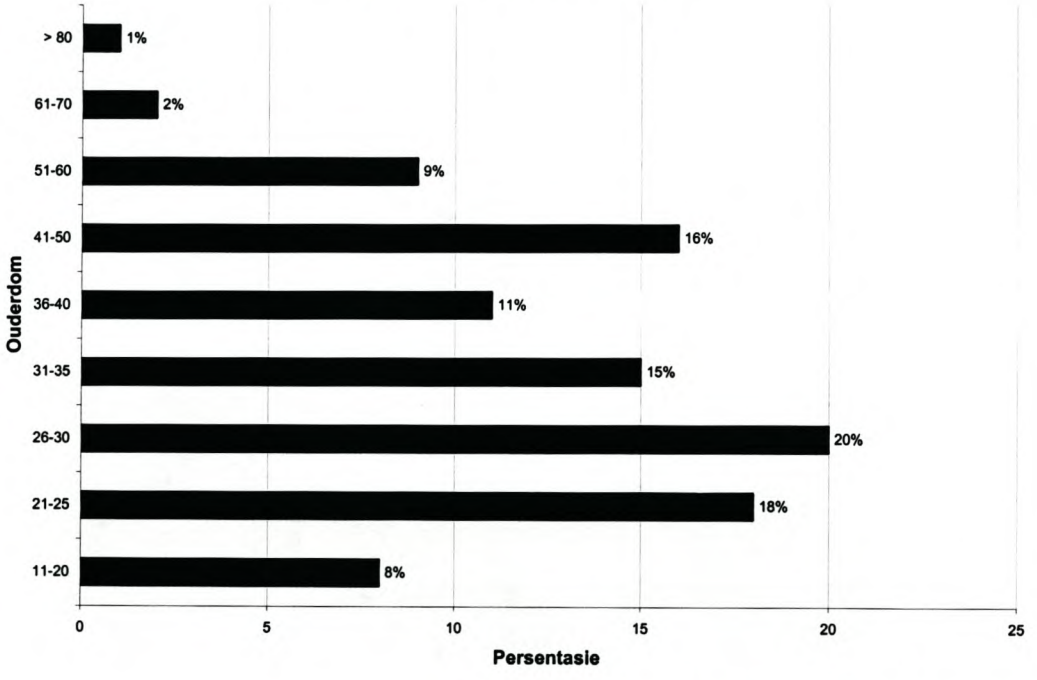
Stellenbosch University http://scholar.sun.ac.za

gebruik Windows95 en gebruik die Internet ewe veel by die huis en die werk. Hy werk moontlik op een of ander wyse in die rekenaarbedryf en gebruik die Internet al vir 'n jaar of twee.

Dié opname word hier bespreek aangesien dit die volledigste Suid-Afrikaanse Internet-gebruikersopname is wat vrylik beskikbaar is. Later in die hoofstuk word die 1997-opname met meer onlangse opnames vergelyk.

Volgens South Africa Online se Suide-Afrikaanse Internet-gebruikersopname van 1997 is die meeste gebruikers tussen 21 en 25 jaar oud, met die meeste gebruikers wat tussen 26 en 30 jaar oud is (sien Tabel 4.1). Dit vergelyk goed met die wêreldwye tendens soos in Tabel 3.3 uiteengesit is, waar die meeste Internet-gebruikers tussen 22 en 35 jaar oud is.

TABEL 4.1: Ouderdom (1997)

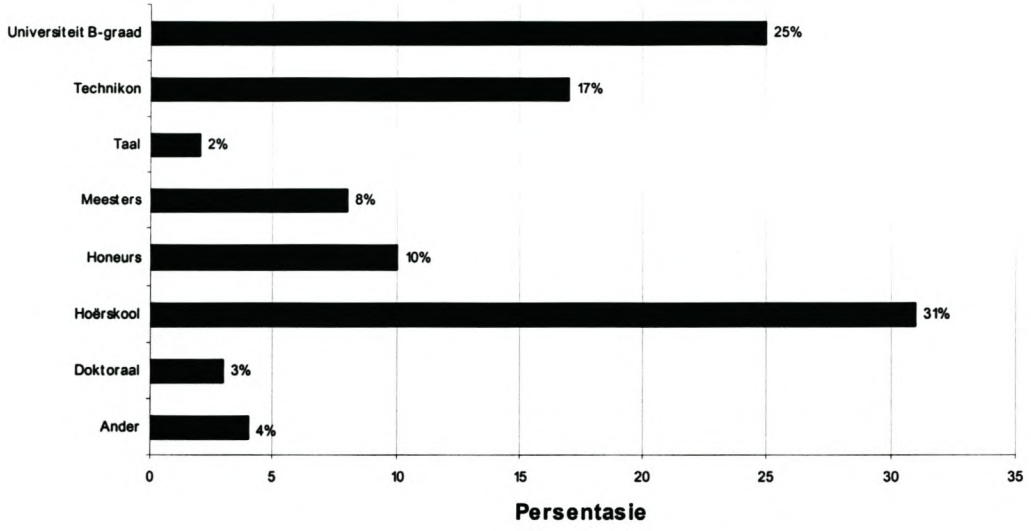


Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Stellenbosch University http://scholar.sun.ac.za

Uit Tabel 4.2 is dit duidelik dat dit meestal mense met 'n mate van opvoeding is wat die Internet gebruik. Die meeste Internet-gebruikers in Suid-Afrika (31%) het 'n hoërskool-sertifikaat, terwyl die grootste groep 'n redelike hoë vlak van opvoeding (Universiteit B-graad, 25% en Technikon 17%) het.

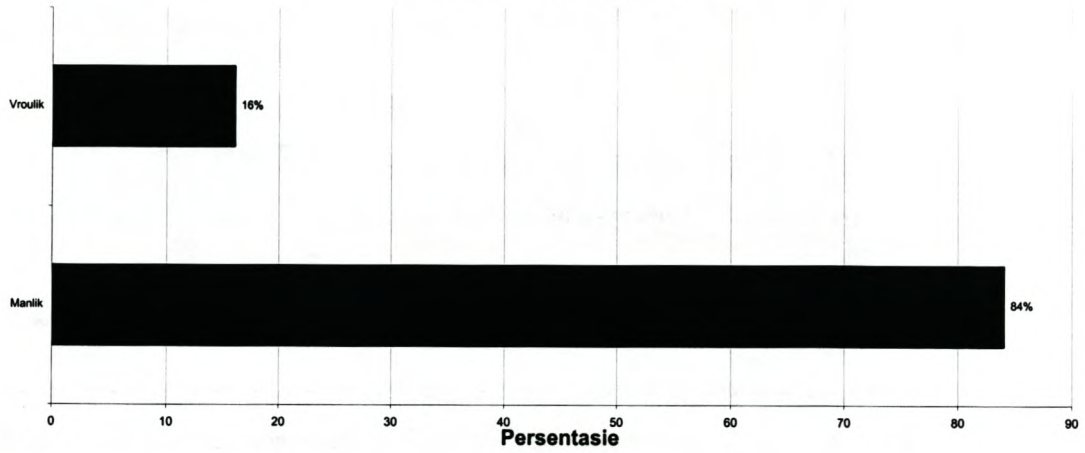
TABEL 4.2: Opvoeding (1997)



Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Soos dit ook wêreldwyd tans die tendens is (sien Tabel 3.4), vorm mans soos in Tabel 4.3 die grootste deel van Internet-gebruikers in Suid-Afrika.

TABEL 4.3: Geslag (1997)

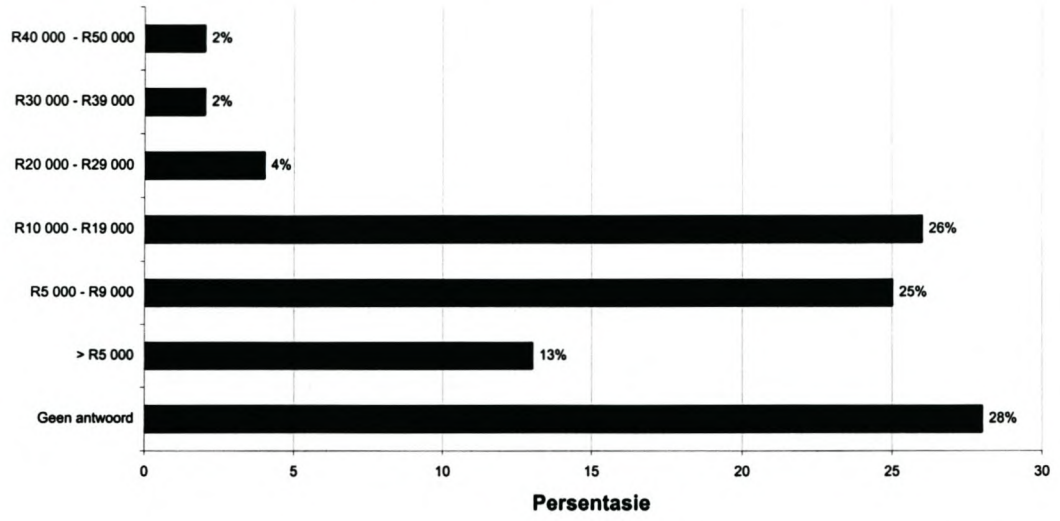


Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Stellenbosch University http://scholar.sun.ac.za

Uit Tabel 4.4 is dit duidelik dat die Internet-gebruikers in Suid-Afrika 'n goeie inkomste verdien. Dit is veral 'n goeie teken vir bemarkers wat aanlyn-aankope moet bemark, omdat hulle nou weet dat die Suid-Afrikaanse Internet-gebruikers 'n besteebare inkomste het.

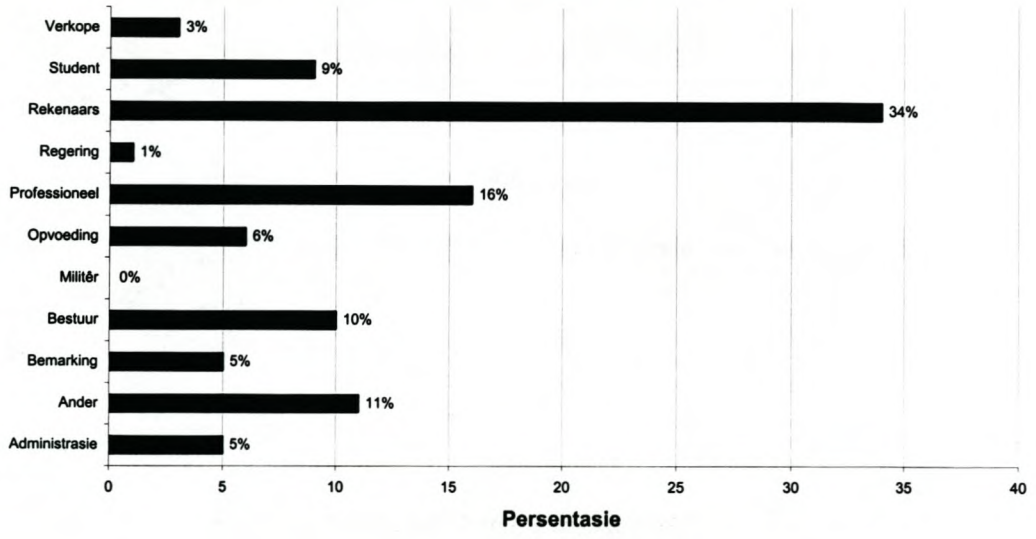
TABEL 4.4: Maandelikse huishoudelike inkomste (1997)



Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Die rekenaarbedryf bly steeds die primêre beroep van Internet-gebruikers (sien Tabel 4.5). Dit is ook wêreldwyd die geval soos reeds in Tabel 3.7 aangedui is.

TABEL 4.5: Primêre beroep (1997)

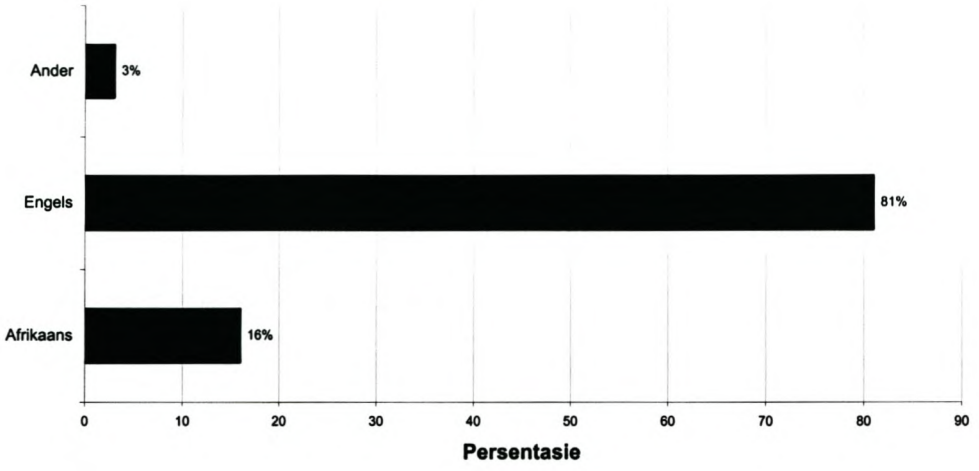


Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Stellenbosch University http://scholar.sun.ac.za

Volgens die 1997 Internet-gebruikersopname van South Africa Online, is meeste Internet-gebruikers in Suid-Afrika Engelssprekend (sien Tabel 4.6). Sedert 1997 het die aantal Afrikaanssprekende gebruikers toegeneem (sien Tabel 4.12).

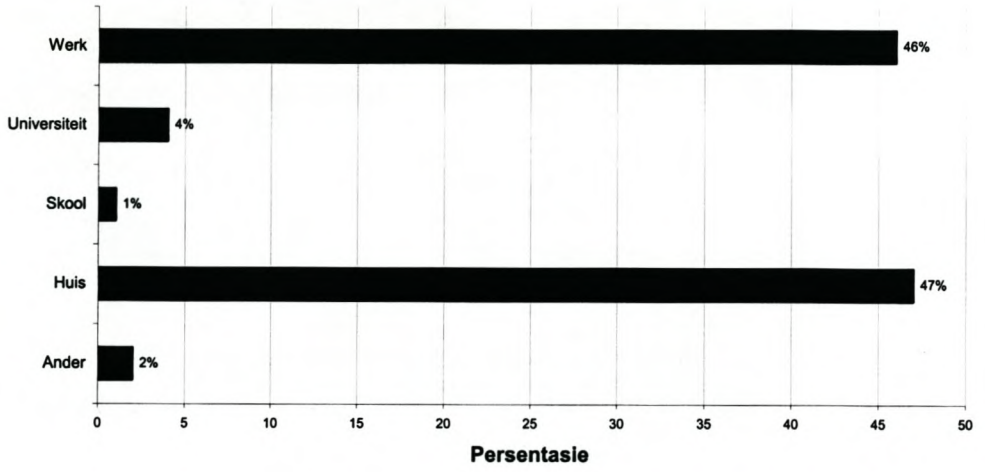
TABEL 4.6: Taal (1997)



Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Die meeste Suid-Afrikaanse Internet-gebruikers kry toegang tot die Internet van die huis of van die werk (sien Tabel 4.7).

TABEL 4.7: Plek van Internet-toegang (1997)

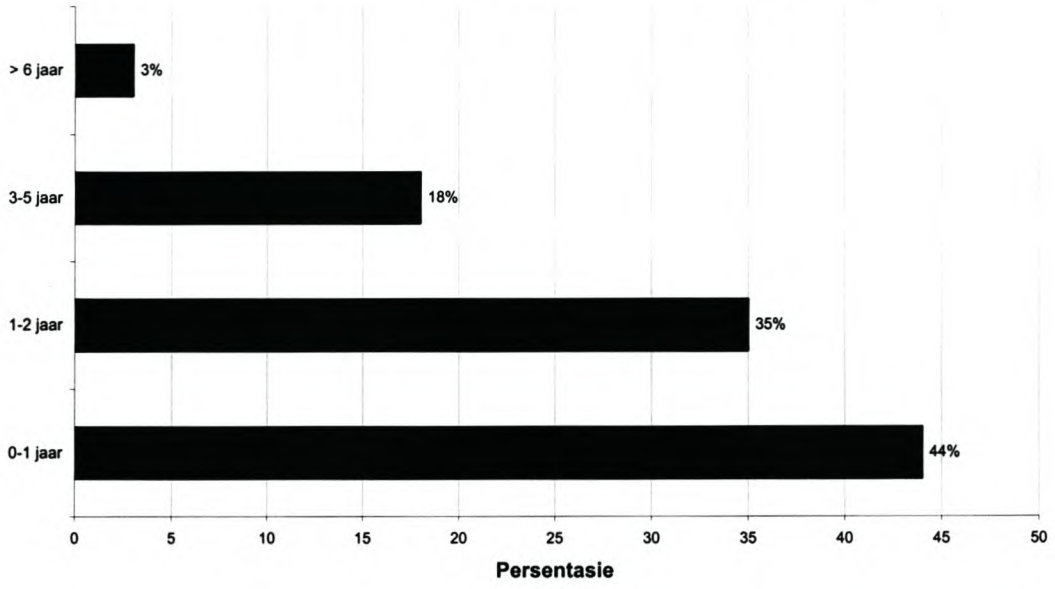


Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Stellenbosch University http://scholar.sun.ac.za

Uit Tabel 4.8 is dit duidelik dat daar min Suid-Afrikaners tydens 1997 was, wat die Internet al vir vyf jaar of langer gebruik. Die meeste mense het pas die Internet begin gebruik of gebruik dit vir so twee jaar al.

TABEL 4.8: Aantal jare Internet gebruik (1997)



Kopiereg 1996, 1997 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

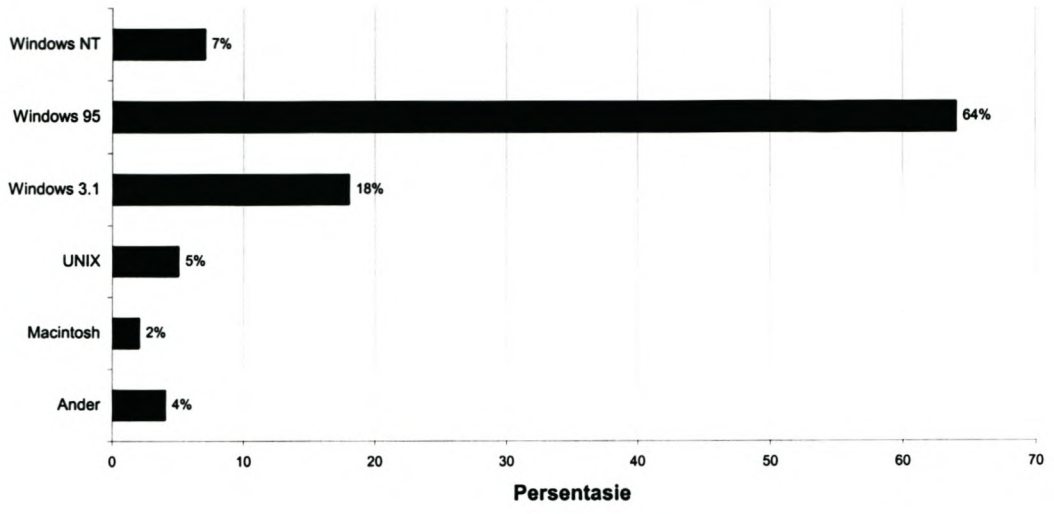
Die meeste Suid-Afrikaanse Internet-gebruikers gebruik Windows 95 as bedryfstelsel vir hul rekenaar (sien Tabel 4.9).

South Africa Online se 1998-opname waaraan 1 400 Suid-Afrikaanse Internet-gebruikers deelgeneem het, verskil nie veel van die tipiese Suid-Afrikaanse Internet-gebruiker wat in die 1997-opname na vore gekom het nie. Tog is daar 'n hele paar interessante syfers wat bespreek moet word.

Die persentasie vroulike Internet-gebruikers het van 16% (1997) verbeter na 19%. Die gemiddelde ouderdom is rondom 35. Die meeste, 35%, val in die 20-30 ouderdomsgroep (1997: 38%), gevolg deur 31-40, 26% (1997: 25%) en 41-50, 21% (1997: 15%). Die sleutelskuif in die ouderdomsgroepe was 'n afname in die 20-jariges en 'n toename by die 40-jariges, wat op die groeiende belangstelling van die Internet by ouer-gebruikers dui.

Stellenbosch University http://scholar.sun.ac.za

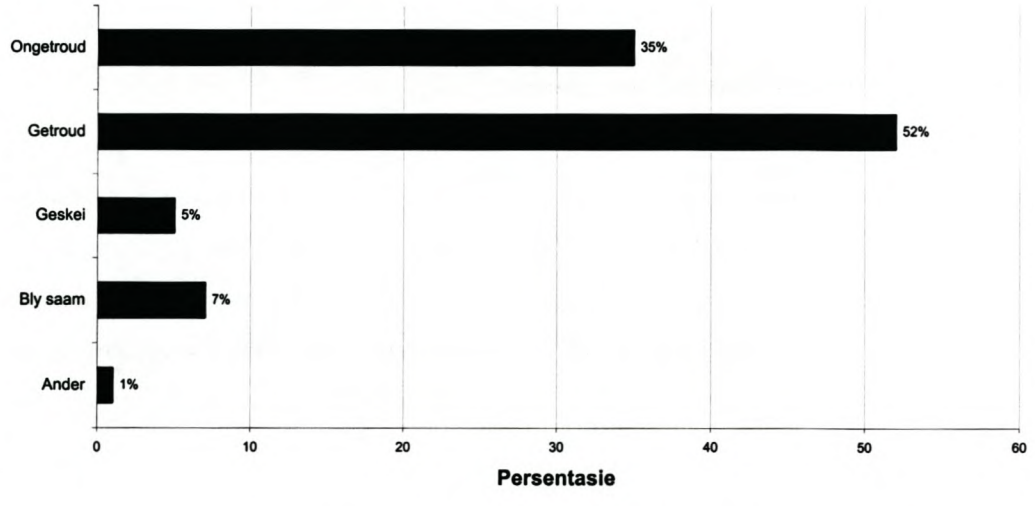
TABEL 4.9: Bedryfstelsel (1997)



Kopiereg 1996, 1997 South Africa Online. All rights reserved
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Die opname het soos in 1997 (sien Tabel 4.10) bevestig dat Internet-gebruikers nie slegs enkellopendes is wat die medium as 'n plaasvervanger vir 'n sosiale lewe gebruik nie. Altesame 56% van die deelnemers aan die opname is getroud of bly saam (1997: 58%). Die aantal ongetroude gebruikers is effens hoër, van 35% in 1997 na 37% in 1998. Die aantal gebruikers wat geskei is, is ook effens hoër na 6% (1997: 4%).

TABEL 4.10: Huwelikstatus (1997)



Kopiereg 1996, 1997 South Africa Online. All rights reserved
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Stellenbosch University http://scholar.sun.ac.za

Die gemiddelde inkomste per huishouding is hoog, teen meer as R11 000 per maand, terwyl die gemiddelde Suid-Afrikaanse Internet-gebruiker hoogs gekwalifiseerd is, met 'n gemiddelde van matriek of een jaar post-matriek studies.

Suid-Afrika volg steeds die wêreldwye tendens in terme van die mees algemene betrekking vir Internet-gebruikers, naamlik die rekenaarbedryf, maar die getal het skerp gedaal. Dieselfde hoeveelheid gebruikers werk nou ook in bestuur, 'n skerp styging sedert 1997. Die syfers dui aan tot watter mate die Internet by 'n hoofstroom gehoor buite die IT-veld aanvaar word.

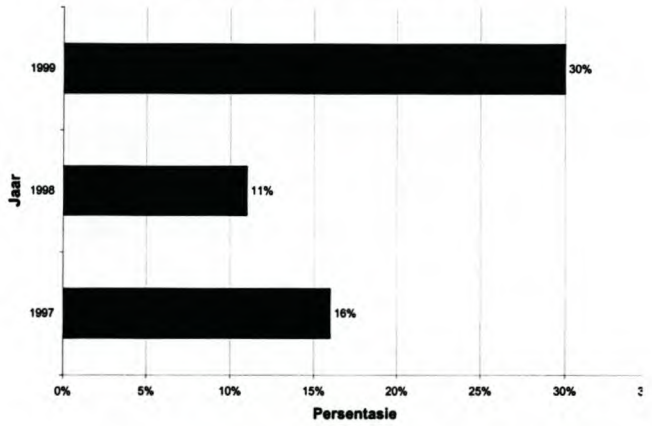
Altesame 81% van die deelnemers aan die 1997-opname het gesê hulle gebruik die Internet elke dag. 'n Stewige 43% van die Internet-gebruikers het al iets aanlyn gekoop. Dis interessant om te sien dat 89% van gebruikers sê hulle beplan om die Internet te gebruik om aankope in die toekoms te doen.

Die meeste van die Internet-gebruikers wat aan South Africa Online se 1998-opname deelgeneem het, gebruik die Internet vir aanlyn-aankope van modems, bedryfstelsels, Internet-blaaier, daaglikse en weeklikse gedrukte koerante en aanlyn nuusdienste (The 1998 South African Web User Survey, 1998).

South Africa Online het in 1999 'n derde Internet-gebruikersopname gedoen waaraan 1 950 Internet-gebruikers deelgeneem het. Volgens die opname dui alles daarop dat die Suid-Afrikaanse Internet-gebruiker al hoe meer ooreenkomste toon met die algemene wêreldwye Internet-gebruiker. Dié ooreenkomste is slegs in terme van die profiel van die Internet-gebruiker en nie die gebruikspatrone van die Internet-gebruiker nie.

Die merkbare tendens is die toename in die aantal vroue wat aan die Internet-gebruikersopname deelgeneem het (sien Tabel 4.11).

TABEL 4.11: Aantal vroue aanlyn

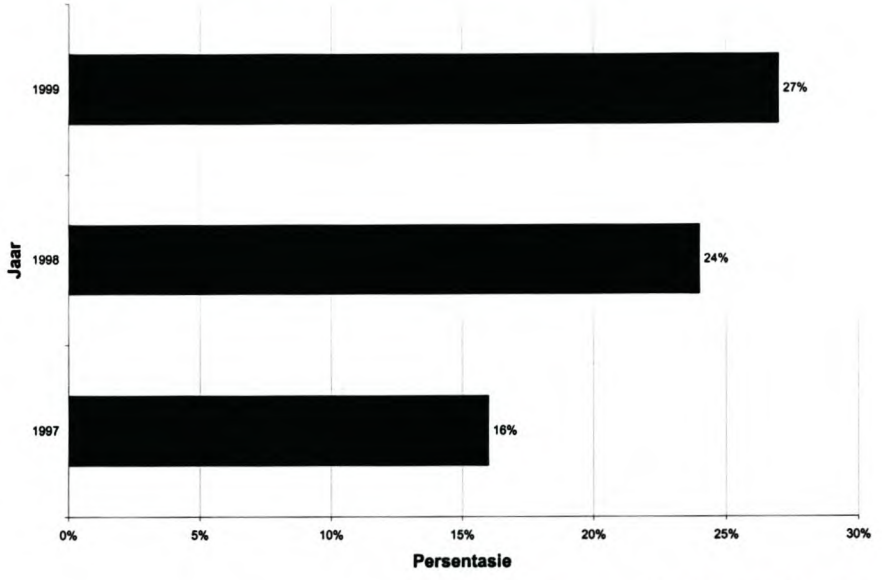


Kopiereg 1996-1999 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Stellenbosch University http://scholar.sun.ac.za

Die aantal Afrikaanssprekende gebruikers het ook toegeneem sedert die eerste Internet-gebruikersopname van 1997 (sien Tabel 4.12).

TABEL 4.12: Afrikaanssprekendes aanlyn



Kopiereg 1996-1999 South Africa Online. All rights reserved;
Bron: The South African Internet User's Survey
(http//:www.southafrica.co.za/survey)

Die gemiddelde inkomste is steeds relatief hoog teen net onder R11 000 per maand met die meeste van die deelnemers aan die opname wat in die rekenaarindustrie werk.

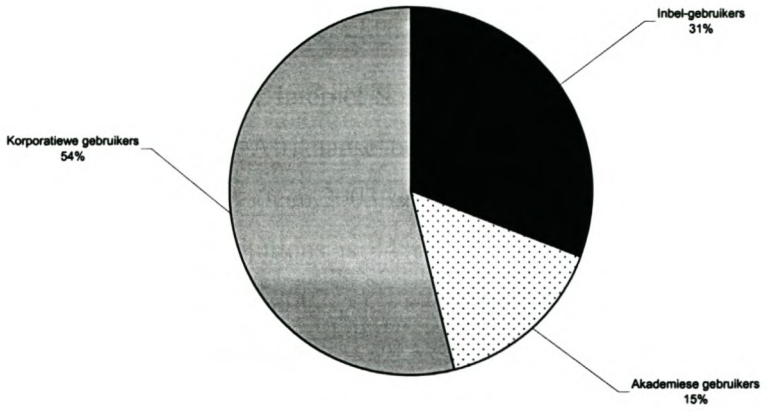
Soos wat verwag is, vorm boeke en CD's die grootste deel van aanlynaankope, maar die aantal mense wat aanlyn-aankope gedoen het, het van 43% in 1998 verminder na 37% in 1999. Daar was ook 'n afname in die hoeveelheid gebruikers wat gesê het hulle beplan om in die toekoms van aanlyn-aankope gebruik te maak (71% in vergelyking met 1998 se 89%). South Africa Online voel dit is deels as gevolg van die invloei van nuwe gebruikers, die relatiewe swak kwaliteit van plaaslike transaksie-webwerwe (in vergelyking met die VSA) en afname in die geweldige ophef wat daar rondom aanlyn-aankope gemaak is (The 3rd South African Web User Survey, 1999).

Volgens 'n onlangse studie deur Internet Solutions (2001) het ongeveer 4% (min of meer 1.8 miljoen gebruikers) van die Suid-Afrikaanse bevolking teen 2000 Internet-toegang gehad. Daar word verwag dat die syfer met 11% teen 2003 sal groei. Die aantal vroue aanlyn is steeds besig om toe te neem. Volgens Internet Solutions is 44% van die Suid-Afrikaanse Internet-gebruikers in 2000 vroue ("South African Usage", 2002: 2).

Stellenbosch University http://scholar.sun.ac.za

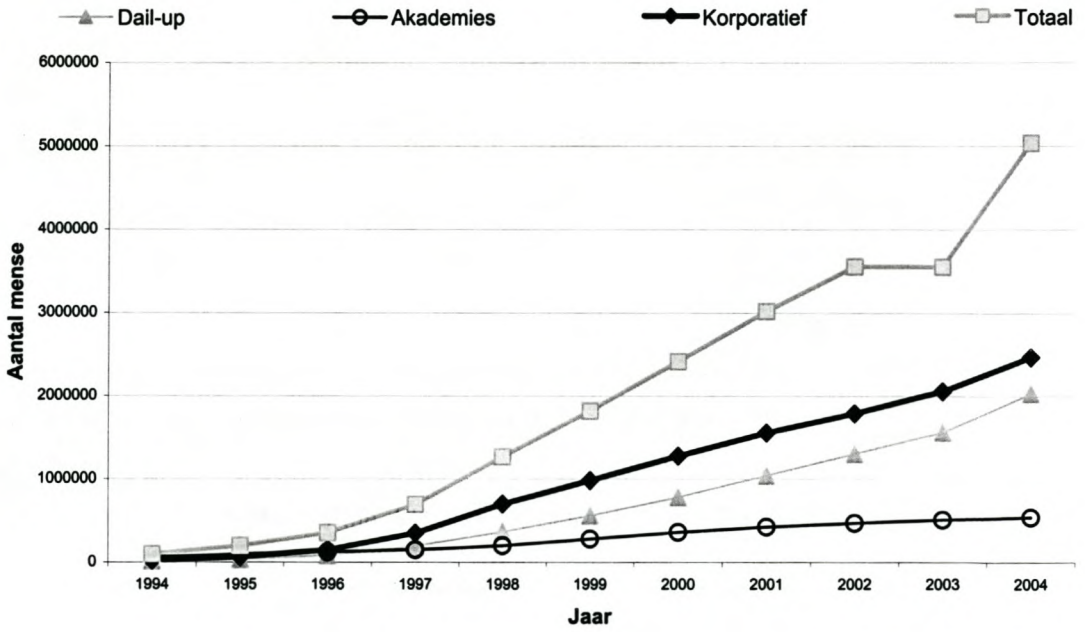
Die Suid-Afrikaanse Internet-gebruikers kan in die volgende kategorieë ingedeel word:

TABEL 4.13: Verskillende Internet-gebruikers in Suid-Afrika (2000)



Internet Solutions het volgens die 4th Internet Services Industry Survey 2000 'n voorspelling gemaak van die Internet-markgroei van 1994 - 2002 (sien tabel hieronder).

TABEL 4.14: Suid-Afrika Internet-markgroei (1994 - 2004)



Stellenbosch University http://scholar.sun.ac.za

4.3 Samevatting

Die ontwikkeling van die Internet in Suid-Afrika het tydens 'n moeilike tydperk in die Suid-Afrikaanse geskiedenis plaasgevind, en aan die voorpunt van dié ontwikkeling was die "liberale" Rhodes Universiteit. Die totstandkoming van 'n volhoubare e-posskakel tussen Rhodes Universiteit en 'n huis in Oregon, VSA word in die algemeen beskou as die begin van die Internet in Suid-Afrika. Weens die politieke situasie in Suid-Afrika in 1989 is toegang tot die wêreldwye Internet egter verbied (Lawrie, 1997:8).

Mike Lawrie wat direkteur van rekenaardienste aan Rhodes Universiteit was en van die begin af by die ontwikkeling van die Internet in Suid-Afrika betrokke was, het in 1990 beheer oor die .za-domeinnaam verkry toe hy dit by Internet Aktiwiteite Raad geregistreer het (Lawrie, 1990:1).

Verskeie bestaande Suid-Afrikaanse wetgewing is deels aangepas om die Internet te akkommodeer, maar die regering het nooit besef wat die werklike impak van die Internet sou wees nie en het gevolglik re-aktief te werk gegaan wanneer dit by die regulering van die Internet gekom het (Buys, 2001: 33). Vanaf 2000 het die regering se Departement Kommunikasie begin met die ontwikkeling van Internet-wetgewing vir die land. In 2002 het die Elektroniese Kommunikasies en Transaksies Wet 25 van 2002 in werking getree.

Die wetsontwerp het baie reaksie uitgelok, sommige positief, ander negatief, maar al die belanghebbendes het saamgestem dat dit nodige wetgewing is, wat al reeds te lank gevat het om te voltooi (Vegter & De Wet, 2002: 29-30).

Daar is min Suid-Afrikaners wat nie deur die Elektroniese Kommunikasies en Transaksies Wet van 2002 geraak sal word nie. Dit is daarom belangrik om te weet hoe die demografie van Internet-gebruikers daaraan uitsien en of Suid-Afrika die wêreldwye tendens volg. Uit die verskillende opnames wat vanaf 1997 onder Suid-Afrikaanse Internet-gebruikers gedoen is, is dit duidelik dat die aantal Suid-Afrikaanse wat die Internet gebruik, steeds toeneem en dat die demografie van die Internet-gebruikers in die land ooreenstem met die wêreldwye tendens ("The 1998 South African Web User Survey", 1998:1).

Aangesien die Suid-Afrikaanse Internet-gebruikersprofiel die tendense volg van die wêreldwye demografie van Internet-gebruikers, is dit belangrik om die wêreldwye tendense in terme van die regulering van die Internet dop te hou. In die volgende hoofstuk word die regulering van die Internet bespreek, met die spesifieke fokus op die regulering van die fisieke struktuur, Internet-rolspelers en wetgewende Internet-organisasies.

Stellenbosch University http://scholar.sun.ac.za

HOOFSTUK 5:
INTERNET-REGULERING

Die Internet is 'n media-vorm wat in wese nie in totaal deur enige gesag gereguleer kan word nie. Regerings sal aanhou probeer om die vryheid wat die Internet bied, te beperk en sal dié nuwe tegnologiese platform vir hulle eie redes soos sensuur en belasting reguleer (Alberts, 2001: 393).

Die Internet kan onderskei word deur sy fisieke struktuur wat die "pype" skep waarin die Internet bestaan en sy inhoud wat bestaan uit die inligting wat 'n Internet-gebruiker sien. In dié hoofstuk sal daar eerstens 'n kort bespreking wees van die regulering van die fisieke struktuur van die Internet. Tweedens sal die verskillende Internet-rolspelers en wetgewende Internet-organisasies bestudeer word. Laastens word daar op drie belangrike reguleringsaspekte gefokus, naamlik kopiereg, handelsmerke en domeinname en kubermisdaad.

5.1 Regulering van die fisieke struktuur van die Internet

Die Internet kan onderskei word deur sy fisieke struktuur wat die pype skep waarin die Internet bestaan en sy inhoud wat bestaan uit die inligting wat 'n Internet-gebruiker sien.

Daar word ook na die fisieke struktuur verwys as die ruggraat van die Internet-bedryf. Die ruggraat is verantwoordelik vir die fisieke verbinding van 'n ontelbare aantal rekenaars met kabels, roeteerders, skakelaars en satelliete regoor die wêreld. Die inhoud van die Internet word van een rekenaar na 'n ander gestuur deur die TCP/IP protokol ("Transmission Control Protocol/Internet Protocol") wat die internasionale sagteware platform is waarvolgens rekenaars opdragte na mekaar kan stuur en ontvang.

Altwee die komponente van die Internet kan tot op 'n sekere punt gereguleer word, aangesien daar beperkinge op die regulering van die Internet is (Alberts, 2001: 393-394).

Die hardeware wat die fisieke boublokke van die Internet vorm, moet êrens in die fisieke of drie-dimensionele wêreld geïnstalleer wees. Die ruggraat van die Internet bestaan op die oomblik uit die volgende:

1. verskeie rekenaars met modems en bedieners in Suid-Afrika en ander lande regoor die wêreld
2. fisieke telefoonkabels (koper of optiese vesel) in Suid-Afrika, in internasionale waters en in ander lande wat elke rekenaar wat aanlyn is met ander regoor die wêreld verbind
3. landelike versenders wat boodskappe van een rekenaar na 'n ander in dieselfde land stuur en ontvang

Stellenbosch University http://scholar.sun.ac.za

4. satelliete wat boodskappe van een rekenaar na 'n ander regoor die wêreld versprei (Alberts, 2001: 395).

Dit is belangrik om te weet hoe die verskillende verbindingsmetodes onderling met mekaar geskakel kan word. Sommige Internet-intekenare kan direk met 'n DTH Sat (*direct-to-home satellite*, wat op dieselfde wyse as satteliet-TV werk) verbind word en hoef dus van geen kabels in hul land of enige ander land gebruik te maak om inligting van 'n rekenaar in 'n ander land te kry nie. 'n DTH Sat-intekenaar kan toegang kry tot 'n aanlyn-rekenaar wat slegs 'n paar blokke ver of selfs 'n paar meter ver is, maar het 'n roete reg oor die wêreld via verskeie kabels en satellietstelsels afgelê om weer in dieselfde land te kom. In sekondes kan so 'n Internet-gebruiker om die wêreld reis en verskeie regstelsels in die kuberruim oorkruis sonder om dit eens te weet (Alberts, 2001: 396).

Die ruggraat van die Internet is inderdaad reeds tot 'n mate deur blote toeval, as gevolg van sy fisieke teenwoordigheid, gereguleer. Die rede hiervoor is dat die ruggraat oorspronklik nie uitsluitlik vir die Internet geskep is nie. Dit was eintlik glad nie vir die Internet geskep nie, maar vir Alexander Graham Bell se groot uitvinding, naamlik die telefoon (Alberts, 2001: 396).

Alle regerings wat telefoon-kommunikasie toegelaat het, het toe al seker gemaak dat daar voldoende regulering vir die nuwe tegnologie binne hul landsgrense was. Dié lande het 'n internasionale regstelsel geskep om die skepping en implementering van universele en uniforme standaarde regoor die wêreld te fasiliteer wat vandag bekend staan as telekommunikasie. Dit is gedoen deur die ontstaan van die Internasionale Telekommunikasie Unie wat 'n amptelike unie van die Verenigde Nasies is (Alberts, 2001: 396).

Die inhoud van die Internet bestaan uit sagteware wat die visuele en oudio-seine skep wat die gebruiker sien en hoor. Daarom is dit maklik om te sê dat die kontraktuele wet wat die gebruik en lisensiëring van sagteware reguleer, die gepaste wet sal wees om die inhoud te reguleer. So ook kan 'n mens aanneem dat die regsnorme wat onder meer kopiereg, handelsmerke en sensorskap reguleer, ook die inhoud en idees wat op die sagteware-platform geplaas word, sal dek. Dit is egter nie so eenvoudig nie, omdat die Internet 'n nuwe vorm van media is wat alle tyds- en geografiese grense ignoreer (Alberts, 2001: 393-397).

Stellenbosch University http://scholar.sun.ac.za

5.2 Internet-rolspelers

Dit is belangrik om te weet wie die Internet-rolspelers is, en wat hulle doen. Die kern van die Internet se infrastruktuur bestaan uit roeteerders, gashere en "pype".

Roeteerders is spesiale-funksie rekenaars of sagteware-pakkette wat die verbinding tussen twee of meer rekenaars hanteer deur na die bestemmingsadres van die pakket-data wat deur hulle beweeg, te kyk en dan te besluit volgens watter roete hulle gestuur moet word.

Gashere is rekenaars wat inligting stoor en dit oor die Internet beskikbaar stel.

Pype is die telekommunikasie-verbindings wat gashere en roeteerders met mekaar skakel en wissel van landlyne tot satellietseine.

Gashere en roeteerders word deur verskeie regeringsorganisasies, private organisasies of individue besit, terwyl pype gewoonlik deur telekommunikasie-ondernemings besit word.

Die volgende Internet-rolspelers sal kortliks bespreek word: Internetdiensverskaffers (IDV's), toegangverskaffers, eweknie-ooreenkomste, gashere, inhoudsverskaffers, navigasie-verskaffers, soek-enjins, transaksie-fasiliteerders, webwerf-ontwerpers en webwerf-skeppers, publieke toegangsverskaffers, webmeesters en portale (Buys, 2001: 19-20).

5.2.1 Internetdiensverskaffers (IDV's)

'n IDV verskaf 'n versameling van dienste, wat onder meer Internet-toegang, gasheer vir inhoud en webwerf-ontwerp insluit. 'n IDV wat 'n gasheer is vir sy kliënte se webwerwe, toegang tot die Internet verskaf, 'n nuusdiens en 'n soek-enjin op sy tuisblad het, vertolk die rol van beide toegangsverskaffer, gasheer, inhoudsverskaffer en navigasie-verskaffer (Buys, 2001: 20).

5.2.2 Toegangsverskaffers

'n Toegangsverskaffer verskaf gebruikerstoegang tot die Internet. Die eerste toegangsverskaffers was akademiese instellings wat hul personeel, fakulteite en studente in staat gestel het om toegang tot die Internet te kry.

Vandag is die tipiese toegangsverskaffer 'n kommersiële organisasie wat Internet-toegang by die huis of aan kommersiële gebruikers verkoop (Buys, 2001: 20-21).

5.2.3 Eweknie-ooreenkomste

Toegangsverkaffers het beide fisieke skakels na en kontraktuele verhoudings met ander toegangsverskaffers en die netwerke wat hulle bedien. Die fisieke verbinding stel die Internet-

Stellenbosch University http://scholar.sun.ac.za

verkeer in staat om deur eweknie-punte tussen twee toegangsverskaffers te beweeg. 'n Eweknie-punt is die gebruik waar ooreenstemmend opgestelde netwerke met mekaar geskakel word waar nie een voorkeur bo die ander geniet nie.

In Suid-Afrika is daar op die oomblik eweknie-punte in Rosebank, Johannesburg (JINX) en Nuweland, Kaapstad (CINX) wat deur ISPA gedryf word en 'n onafhanklike eweknie-punt wat deur TENET ("Tersiary Education Network") gedryf word (Buys, 2001: 21).

Die kontraktuele ooreenkomste word eweknie-ooreenkomste genoem en reguleer die wisseling van inligting tussen die deelnemende toegangsverskaffers se netwerke. In 'n tipiese ooreenkoms sal daar staan dat nie een van die deelnemers die gebruik van die inligting op hul netwerk mag beperk nie of sulke inligting filtreer voor die versending of ontvangs nie.

As daar geen direkte fisieke verbinding of eweknie-ooreenkoms tussen twee netwerke is nie, moet die Internet-verkeer 'n ander roete vind (Buys, 2001: 21).

5.2.4 Gashere

Gebruikers kry deur die Internet toegang tot data wat op 'n gasheer-rekenaar gestoor word. Die data kan verskillende vorme aanneem - van sagteware tot webwerwe met teks, grafika, oudio, video en ander databasisse. 'n Gasheer kan ook as 'n stoorplek dien vir USENET nuusgroepe of vir die stoor van e-pos in posbusse vir intekenare.

Daar moet egter onderskei word tussen die eienaarskap van die gasheer-rekenaar, die eienaarskap van die inhoud en gasheer-kontrakte.

'n Gasheer kan sy eie data stoor of data vir ander partye stoor, gratis of as 'n kommersiële diens. Die data kan permanent of kortstondig wees. Die eienaar van die gasheer-rekenaar mag aktief betrokke wees by die proses om die data op die gasheer-rekenaar te plaas, of mag dalk niks daarmee te doen hê nie.

Die verantwoodelikheid en verpligtings van die gasheer-eienaar sal verskil volgens die tipe rol wat hy aanneem. In elke moontlike situasie sal die verhouding tussen die eienaar van die rekenaar en die data wat op die gasheer gestoor word, ondersoek en getoets word.

In gevalle waar die eienaar van die gasheer-rekenaar nie die eienaar van die inhoud is nie, sal daar 'n kontrak tussen die twee partye opgestel word. So 'n kontrak moet twee belangrike punte aanspreek:

1. Die gasheer is die storingsmeganisme waarin die inhoud van die webwerf gehou word.
2. Die gasheer is verbind tot die Internet en verskaf 'n buis waardeur gebruikers toegang tot die webwerf kan kry (Buys, 2001: 22-24).

Stellenbosch University http://scholar.sun.ac.za

5.2.5 Inhoudsverskaffers

Inhoudsverskaffers is waarskynlik die belangrikste bydraers tot die Internet, omdat hulle die beskikbare data en informasie verskaf. Groot ondernemings, regerings en individue kan almal inhoudsverskaffers wees. Die inhoud wat hulle verskaf, is beskikbaar in verskeie vorme - daar is inligting op die Internet wat elke moontlike onderwerp dek (Buys, 2001: 24).

5.2.6 Navigasie-verskaffers

'n Algemene klagte van Internet-gebruikers is dat die inhoud volgens hoeveelheid en nie kwaliteit van mekaar onderskei word nie. Selfs al is daar kwaliteit-inhoud beskikbaar is dit nie maklik om te vind nie of om die kwaliteit van die inhoud te assesseer nie.

Navigasie-verskaffers speel 'n belangrike rol om die nuttelose inhoud van die bruikbare inhoud te onderskei (Buys, 2001: 25). 'n Voorbeeld van 'n navigasie-verskaffer is die Franse webwerf, www.bonweb.com.

5.2.7 Soek-enjins

Op die oomblik is die belangrikste navigasie-verskaffers soek-enjins en Internet-gidse. Hulle katalogiseer die Internet hulpbronne sodat die gebruiker óf 'n kernwoord-soektog of 'n frase-soektog vir die relevante webwerwe dan doen.

Dié tipe eerste-generasie soek-enjins sit kernwoorde op die indeks wat deur die inhoudsverskaffers verskaf is wat meestal misleidend is, omdat hulle ingesluit is om 'n beter plek op die ranglys van die soek-enjin te kry. 'n Bekende eerste-generasie soek-enjin is www.altavista.com.

Tweede-generasie soek-enjins het meer beheer oor die proses van die indekslys en probeer om tussen die kwaliteit van die inhoud te onderskei (Buys, 2001: 25). *AskJeeves* is 'n tipe tweede-generasie soek-enjin wat by www.ask.com beskikbaar is.

5.2.8 Transaksie-fasiliteerders

Die toename in e-handel op die Internet het investering op die Internet gestimuleer om sodoende tekortkominge te oorkom. Om die probleemareas soos sekuriteit aan te spreek, het transaksie fasiliteerders verskeie sekuriteits- en digitale handskrif-produkte gelisensieer en gepatenteer (Buys, 2001: 26).

Stellenbosch University http://scholar.sun.ac.za

5.2.9 Webwerf-ontwerpers en -skeppers

Webwerf-ontwerpers en -skeppers word deur inhoudsverskaffers gebruik. As 'n afsonderlike ontwerpagentskap gebruik word, moet die kontrak tussen die betrokke partye die vraag van eienaarskap van intellektuele eiendom beantwoord. Die kopiereg moet verkieslik aan die inhoudsverskaffer toegeken word.

Die kontrak vir die skep van die webwerf moet dieselfde wees as 'n sagteware-ontwikkelingsooreenkoms. Die inhoudsverskaffer moet toegelaat word om aanvaardingstoetse te doen. Soos met die ontwerp van die webwerf moet die saak van eienaarskap van die intellektuele eiendomsreg aangespreek word (Buys, 2001: 26-27).

5.2.10 Publieke toegangsverskaffers

Sommige ondernemings en organisasies bied publieke toegang tot die Internet aan deur kliënte toe te laat om die rekenaars wat by 'n spesifieke plek aan die Internet verbind is, te gebruik, soos bv. Internet-kafees. Gebruikers betaal gewoonlik vir die dienste per uur (Buys, 2001: 27).

5.2.11 Webmeesters

'n Webmeester is 'n individu wat die webwerf bestuur. Die persoon kan 'n werknemer van 'n onderneming wees wat 'n webwerf besit of kan in sy persoonlike hoedanigheid optree. Afhangende van die grootte van die webwerf, kan die webmeester verantwoordelik wees vir die hardeware en sagteware, ontwerp en instandhouding van die webwerf, opdatering van die webwerf, terugvoer aan gebruikers gee en die verkeer na die webwerf monitor (Buys, 2001: 27).

5.2.12 Portale

'n Portaal is 'n webwerf wat heel eerste verskyn as 'n persoon sy Internet-blaaier aktiveer. Dié webwerwe het gewoonlik 'n nuus-afdeling, soek-fasiliteit en die dag se weer (Buys, 2001: 27).

5.3 Wetgewende Internet-organisasies

Daar is verskeie wetgewende Internet-organisasies, maar in die afdeling sal slegs die volgende organisasies kortliks bespreek word, wie hulle is en wat hulle doen: W3C (World Wide Web Consortium), ISOC (The Internet Society), ICANN (The Internet Corporation for Assigned Names and Numbers), die Nasionale Arbitrasie Forum van die VSA en WIPO (World Intellectual Property Forum).

Wetgewende Internet-organisasies in Suid-Afrika word in Hoofstuk 6 bespreek.

Stellenbosch University http://scholar.sun.ac.za

5.3.1 W3C (World Wide Web Consortium)

Die W3C is 'n internasionale organisasie wat hom toespits op die Wêreldwye Web. Sy werk word verdeel tussen vier werkgroepe - die gebruikers-koppelvlakgroep, die tegnologie en gemeenskaps-groep, die argitektuurgroep en die web-toegangsinisiatief (Buys, 2001: 28).

Die W3C ontwikkel spesifikasies, riglyne, sagteware en gereedskap om die www tot sy volle potensiaal te lei ("Leading the Web", 2002:1).

Die gebruikerskoppelvlakgroep is verantwoordelik om toe te sien dat die www se funksionaliteit verbeter, maar dat alles so eenvoudig moontlik bly.

Die tegnologie en gemeenskapgroep konsentreer op sake wat ontstaan uit die toepassing en gebruik van die www.

Die argitektuurgroep van W3C kyk na die toekoms en lei die evolusie van die www deur onder meer te konsentreer op die samelopende sake en die integrasie van die www en televisie-tegnologie (Buys, 2001: 28).

5.3.2 ISOC (The Internet Society)

ISOC is in 1992 gestig en sy hoofkantoor is in Reston, Virginia, VSA. Dit dien as 'n internasionale organisasie vir globale koördinasie en samewerking op die Internet. ISOC bevorder 'n wye reeks aktiwiteite wat op die Internet se ontwikkeling en beskikbaarheid en soortgelyke tegnologieë gefokus is (Buys, 2001: 28).

ISOC het 'n professionele lidmaatskap van meer as 150 organisasies en 11 000 individuele lede in meer as 182 lande. Die vereniging se individuele en organisasielede word deur die algemene aandeel om die lewensvatbaarheid van die Internet te onderhou, verbind. Hulle bestaan uit die ondernemings, regeringsinstansies en stigtings wat die Internet en sy tegnologieë geskep het ("All About the Internet Society", 2002).

ISOC is ook die organisatoriese tuiste vir die groepe wat verantwoordelik is vir die Internet-standaarde, naamlik die IETF (Internet Engineerings Task Force), die IAB (Internet Architecture Board) en IANA (Internet Assigned Numbers Authority).

Die IETF hou hom besig met die argitektuur en die vloeiende werking van die Internet. Die IAB is 'n tegniese raadsgroep wie se verantwoordelikhede die algemene argitektuur van die Internet soos die ruggrate en al die netwerke wat hulle verbind, insluit. IANA lei die organisasies wat verantwoordelik is om IP-adresse toe te ken (Buys, 2001: 28).

Stellenbosch University http://scholar.sun.ac.za

5.3.3 ICANN (The Internet Corporation for Assigned Names and Numbers)

ICANN is 'n tegniese koördinerende liggaam vir die Internet. Dit is in Oktober 1998 gestig deur 'n breë koalisie van Internet-ondernemings, tegniese-, akademiese-, en gebruikersgemeenskappe.

ICANN neem verantwoordelikheid vir 'n stel tegniese funksies wat voorheen deur die Amerikaanse regering se kontrak met IANA en ander groepe uitgevoer is. Dié organisasie is spesifiek verantwoordelik vir die koördinering van die volgende indentifiseerders wat wêreldwyd uniek moet wees, om die Internet te laat funksioneer:

1. Internet domein-name
2. IP-adresnommers
3. Protokol parameter en poortnommers

ICANN is verder ook verantwoordelik vir die koördinasie van die stabiele werking van die Internet se stambedieningstelsel ("root server system"). ICANN se UDRP (Domain-Name Dispute Resolution) word by punt 4.4.4 later in die hoofstuk bespreek ("The Internet Corporation for Assigned Names and Numbers, 2002).

5.3.4 Nasionale Arbitrasie Forum

Die Nasionale Arbitrasie Forum van die VSA is een van die vernaamste Internet domeinnaam-dispuutresolusie-verskaffers in die wêreld en die grootste verskaffer van domeinnaam-dispuutresolusies in Noord-Amerika. Saam met die forum se oplossings van domeinnaam-dispute deur middel van die ICANN UDRP verskaf die forum ook 'n verskeidenheid dienste onder die nuwe domein-uitbreidings vir .biz, .info, .name, .us en vir new.net domeinname.

Hier is 'n lys van die verskillende dispuutresolusie-beleide wat die Nasionale Arbitrasie Forum gebruik:

1. **UDRP (Uniform Domain Name Dispute Resolution Policy)** is die oorspronklike dispuutresolusie prosedure wat deur ICANN in 1999 aangeneem is.
2. **STOP (Start-up Trademark Opposition Policy for .BIZ)** sal deur handelsmerk-eienaars wat voorheen 'n IP Claim by Neulevel, Inc. gemaak het, gebruik word.
3. **RDRP (Restrictions Dispute Resolution Policy for .BIZ)** kan deur enigeen gebruik word wat die onderneming of kommersiële doel van 'n .biz domeinnaam wil uitdaag.
4. **ERDRP (Eligibility Requirements Dispute Resolution Policy for .NAME)** kan deur enigeen gebruik word wat die geskiktheid van 'n geregistreerde .name domeinnaam wil uitdaag.
5. **usDRP (usTLD Dispute Resolution Procedure for .US)** kan deur partye gebruik word wat die registrasie van .US domein-name bevraagteken.

Stellenbosch University http://scholar.sun.ac.za

6. **usNDP (usTLD Nexus Dispute Procedure for .US)** kan deur partye gebruik word wat 'n geregistreerde .us domeinnaam se nakoming van die usTLD Nexus vereistes wil bevraagteken.
7. **MDRP (Model Domain Name Dispute Resolution Policy)** kan deur partye gebruik word wat die registrasie van 'n New.net domeinnaam wil bevraagteken ("National Arbitration Forum: Domain Dispute", 2002).

5.3.5 WIPO (World Intellectual Property Organization)

WIPO is 'n internasionale organisasie wat die gebruik en beskerming van intellektuele eiendom bevorder. Met sy hoofkantoor in Geneva, Switzerland, is WIPO een van die Verenigde Nasies se spesialis-agentskappe wat 23 internasionale verdrae administrateer. Daar is 179 lidland verbonde aan WIPO, waarvan Suid-Afrika een is.

Die begin van WIPO dateer van 1883 toe die Parys Konvensie vir die beskerming van Industriële Eiendom in werking getree het. Dit was die eerste internasionale verdrag wat geskep is om mense van een land te help om beskerming van hu intellektuele eiendom in ander lande te verkry. In 1884 het die 14 lidland van die Parys Konvensie 'n internasionale buro saamgestel om die administratiewe sake van die lidlande te hanteer. In 1893 is BIRPI ("United International Bureaux for the Protection of Intellectual Property" - algemeen bekend as BIRPI, sy Franse akkroniem) tot stand gebring, wat die voorganger van WIPO was. WIPO is in 1970 gestig na die WIPO Konvensie in 1967 ("About WIPO", 2003: 4).

Die doel van WIPO is om:

1. nasionale intellektuele eiendomsregulering met internasionale regulering te harmoniseer;
2. dienste vir internasionale aansoeke vir industriële eiendomsregte te verskaf,
3. intellektuele eindom inligting uit te ruil,
4. regs- en tegniese hulp aan ontwikkellende en ander lande te verskaf,
5. die resolusie van private intellektuele eiendom dispute te fassiliteer ("About WIPO", 2003: 4).

Stellenbosch University http://scholar.sun.ac.za

5.4 Kopiereg

Dean (soos aangehaal in Buys, 2001: 40) definieer kopiereg as:

> "die eksklusiewe reg wat betrekking het op werk wat intellektuele inhoud (i.e. die produk van die intellek) insluit om te doen of ander te bemagtig om sekere aksies met betrekking tot die werk te doen, watter handelinge elke tipe werk verteenwoordig, die wyse waarop die werk ontgin kan word vir persoonlike wins of vooruitgang ".

Elke land het sy eie wette wat kopiereg, handelsmerke, patente, ontwerpe en handelsname reguleer, maar enigeen wat iets op die Internet publiseer, kan wette enige plek in die wêreld oortree. Die aard van die Internet sal lande dwing om wetgewing te standaardiseer, nie net in die intellektuele eiendomsveld nie, maar ook op ander plekke.

Op die oomblik word internasionale verhoudings in die intellektuele eiendomsveld in Suid-Afrika deur verskeie internasionale konvensies en ooreenkomste gereguleer. Die vernaamste is die Bern Konvensie op Kopiereg, die Parys Konvensie en die Ooreenkoms oor Handelsverwante Aspekte van Intellektuele Eiendomsreg (TRIPS). Die konvensies en veral die TRIPS ooreenkoms maak sommige regulering van die oortreding van intellektuele eiendomsreg oor grense moontlik deur die ondergetekendes te dwing om buitelandse werk deur die wysiging van hul plaaslike wetgewing te beskerm.

Kopiereg is die intellektuele eiendomsreg wat die meeste deur die Internet bedreig word. Die digitalisering van werke, insluitende geskrewe tekste, grafika, foto's, tekeninge, musiek en video-snitte, het die kopiëring en verspreiding van dié werke byna sonder inspanning, onmiddellik en perfek moontlik gemaak. Dit kan teen die minimum onkoste gedoen word.

Die feit dat tegnologie dit maklik maak om goed te kopieer, beteken nie dat kopiereghouers hul kopiereg prysgee wanneer werke op die Internet of deur iemand anders op die Internet geplaas word nie.

Deur hul werk op 'n webwerf te plaas, moet kopiereghouers vanselfsprekend 'n nie-eksklusiewe lisensie aan alle Internet-gebruikers wat toegang tot die materiaal het, toeken sodat kortstondige kopieë van die materiaal op hul rekenaars gemaak kan word. Dit is nodig omdat die rekenaar van 'n Internet-gebruiker wat die toegang tot die webblad kry, 'n kopie van die materiaal op sy RAM (ewetoeganklike geheue – "random access memory") maak sodat die inhoud op sy rekenaarskerm kan verskyn (Buys, 2001: 37-38).

Stellenbosch University http://scholar.sun.ac.za

Tegnologie self sal die beste manier wees om kopiereg op die Internet te beskerm (Buys, 2002: 39). DRM-sagteware (Digital rights management) is 'n voorbeeld van die tegnologiese ontwikkeling wat die kopiereghouer beskerm. Van die DRM-sagteware enkodeer die kopiereg-materiaal sodat dit nie afgelaai, gekopieer of gestuur kan word sonder om daarvoor te betaal nie (Levine, 2001: 66).

Kopiereg gee die eienaar eksklusiewe regte om die kopieregte werk of dele daarvan te beheer, te gebruik en te bewerk (Buys, 2002: 39).

Sien hoofstuk 6 vir meer inligting oor kopiereg en kopiereg-wetgewing in Suid-Afrika.

5.4.1 Internet-kopiereg: probleemareas

Die Internet skep unieke voorbeelde van kopiereg-oortredings wat probleme regoor die wêreld veroorsaak. Die verskillende probleemareas wat bespreek sal word, is verbindings, rame, voorlopige berging ("caching"), spieël-webwerwe en derde-party aanspreeklikheid.

■ Verbindings

Die fondament van die Internet is sy stelsel van hiperskakels wat die gebruiker toelaat om moeiteloos van die een webwerf na die ander te beweeg. Daar is twee soorte hiperskakels wat algemeen gebruik word, nl. uitskakels ("out links") en inskakels ("in links").

Deur 'n uitskakel te aktiveer, word 'n gebruiker oorgeplaas van die dokument waarna hy gekyk het, na 'n ander dokument êrens anders op die Internet. Die tweede dokument kan 'n ander deel van dieselfde webbladsy wees, of êrens anders op die webwerf of 'n heel ander webwerf. Die gebruik van 'n uitskakel sal nie 'n kopie maak van die dokument waarna dit skakel op die webwerf wat die uitskakel bevat nie.

Die tweede soort skakel (inskakels) word op webwerwe gebruik wat bekend staan as metawerwe ("metasites"). Die doel van die inskakel is om inhoud van die webwerf waarna dit skakel, te kry, wat dan deel word van die webwerf waarop die skakel vertoon word. Die inskakel maak 'n kopie van die inhoud op die webwerf waarop dié skakel is.

In die geval van 'n uitskakel sal die gebruiker na die webwerf gaan waarna daar geskakel word en dié webwerf se URL (uniforme hulpbronadres) vertoon. Met 'n inskakel verlaat die gebruiker nie die webwerf waarop die skakel is nie. In plaas daarvan word die inhoud wat van die geskakelde webwerf verkry word, as deel van die webwerf met die inskakel op vertoon sonder dat die URL verander.

Stellenbosch University http://scholar.sun.ac.za

In albei gevalle vermy die webwerf met die uit- of inskakels daarop om kopieë van die inhoud van die geskakelde webwerf op sy eie stelsel te maak, hoewel daar in die geval van 'n inskakel 'n kopie van die inhoud op die gebruiker se rekenaar gemaak word.

Is die voorsiening van 'n ongemagtigde skakel 'n vorm van kopiereg-oortreding?

Een van die verwere teen aanklagte van kopiereg-oortreding is dat alle webwerf-eienaars een gemeenskaplike doel voor oë het, en dit is om seker te maak dat die maksimum aantal gebruikers hul webwerwe gebruik. Deur 'n skakel na 'n ander webwerf te skep, sonder dié webwerf-eienaar se medewete, is nie nadelig vir die webwerf nie, omdat dit die verkeer na daardie webwerf vermeerder. Die voortbestaan van die Internet berus op webwerwe wat na ander webwerwe deur middel van uitskakels, sonder die nodige bemagtiging, kan skakel.

Die argumente stel 'n sterk saak dat hiperteksskakels in die algemeen sonder die nodige toestemming toegelaat moet word. Daar is egter sekere maniere waarop hiperskakels gebruik word wat nadelig vir die teiken-webwerf kan wees.

Die saak *Ticket Master Corporation v. Microsoft Corporation* waarin Microsoft 'n stadsgids-webwerf oor Seattle bedryf, is 'n voorbeeld van 'n saak waar uitskakels betrokke is en waar kopiereg verbreek is. Microsoft het uitskakels na Ticket Master se webwerf en na die webblaaie waar gebruikers die betrokke kaartjies vir 'n konsert kon koop, gebruik sonder hul toestemming (Buys, 2001: 55-58).

■ Rame

HTML-tegnologie maak dit vir die eienaar van 'n webwerf moontlik om die webwerf in 'n aantal aparte areas of vensters in te deel sodat elkeen afsonderlik beheer kan word. Raamstelsels, waar een webwerf as deel van 'n ander geïnkorporeer word, is ook moontlik. 'n Inskakel word gebruik om met die betrokke webwerf te skakel sonder om die gebruiker se verbinding met die oorspronklike webwerf te verbreek. Die stelsel word ook gebruik om metawerwe saam te stel soos reeds hierbo verduidelik is (Buys, 2001 59-60).

■ Voorlopige berging

Die doel van voorlopige berging is om die Internet vinniger en meer doeltreffend te maak. 'n Kasgeheue ("cache") is die voorlopige berging op die plaaslike geheue van elektroniese kopieë van die werk wat van verwyderde webwerwe verkry is. Dit kan op die hardeskyf van die gebruiker se rekenaar gemaak word, of in die geheue van die storingsfasiliteite van die Internet-diensverskaffers.

Stellenbosch University http://scholar.sun.ac.za

Die proses van voorlopige berging is altyd 'n potensiële oortreding omdat daar altyd kopieë gemaak word. Daar word egter algemeen aanvaar dat voorlopige berging noodsaaklik is vir die doeltreffende gebruik van die Internet. Dit kan as deel van die webwerf-eienaar se onvoorwaardelike ooreenkoms met alle Internet-gebruikers wees, waarna vroeër verwys is (Buys, 200: 60).

Roux de Villiers skryf in Cyberlaw@SA (2001: 61) dat daar geen rede is waarom reserwe-kopieë van 'n gedeelte van 'n webwerf nie toegelaat mag word nie. De Villiers glo dié soort rugsteunkopie is nie so verskillend van 'n rugsteunkopie van 'n gewone rekenaarprogram nie en is noodsaaklik vir die Internet om doeltreffend te funksioneer.

- **Spieël-webwerwe**

Spieël-webwerwe verskil van kasgeheue in die sin dat elke spieël-webwerf uit 'n aparte webwerf bestaan, al kan hulle deur dieselfde URL bereik word. Spieël-webwerwe word gewoonlik deur dieselfde eienaar geskep, maar by verskillende plekke in die wêreld, om meer doeltreffende toegang tot die webwerf te verseker. Dit sal baie moeilik wees vir die skepper van 'n ongemagtigde spieël-webwerf om te verduidelik dat dié webwerf binne die onvoorwaardelike ooreenkoms wat webwerf-eienaars aan gebruikers toestaan, val (Buys, 2001: 61-62).

- **Derdeparty aanspreeklikheid**

'n Persoon wat iemand anders toelaat of veroorsaak om sy/haar Internet-diens te gebruik om oortredingskopieë van kopiereg-materiaal te maak, is ook verantwoordelik vir die oortreding. Dit is vanselfsprekend ook van toepassing op IDV's en gashere wat dit bewustelik doen, maar is ook van toepassing as hulle glad nie daarvan bewus is nie.

Soms is dit baie moeilik om die persoon wat direk vir die oortreding verantwoordelik is, vas te trek, veral met die gebruik van bulletinborde op die Internet (Buys, 2001: 62).

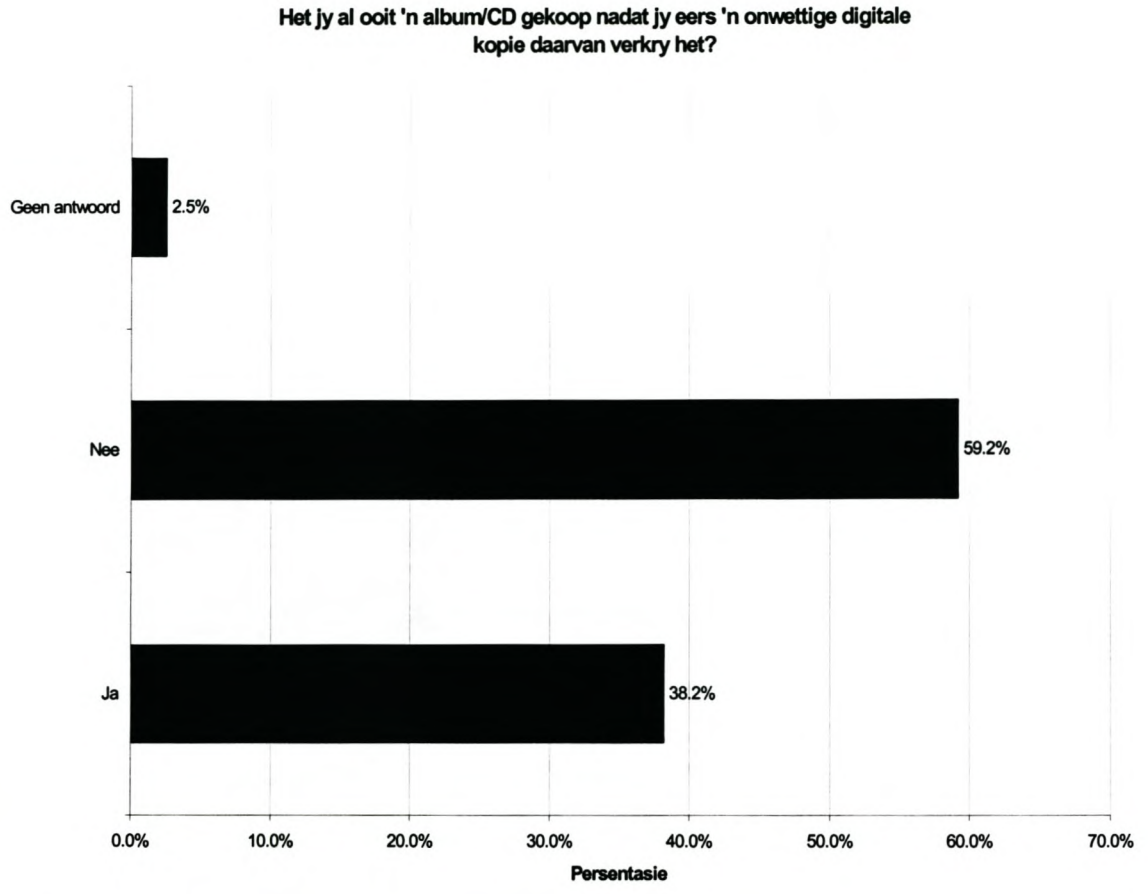
5.4.2 Aanlyn Intellektuele eiendom-opname

Survey.net het in Mei 2002 'n intellektuele eiendom-opname gedoen waaraan 1 807 Internet-gebruikers deelgeneem het. Dit is interessant om te sien hoeveel Internet-gebruikers al kopiereg op die Internet oortree het en hoe min agting hulle vir kopiereg het ("Online Intellectual Propery", 2002:1).

Stellenbosch University http://scholar.sun.ac.za

In Tabel 5.1 het 59,2% van die Internet-gebruikers wat aan die opname deelgeneem het, aangedui dat hulle nooit 'n CD gekoop het nadat hulle eers 'n onwettige digitale kopie daarvan verkry het nie.

TABEL 5.1:

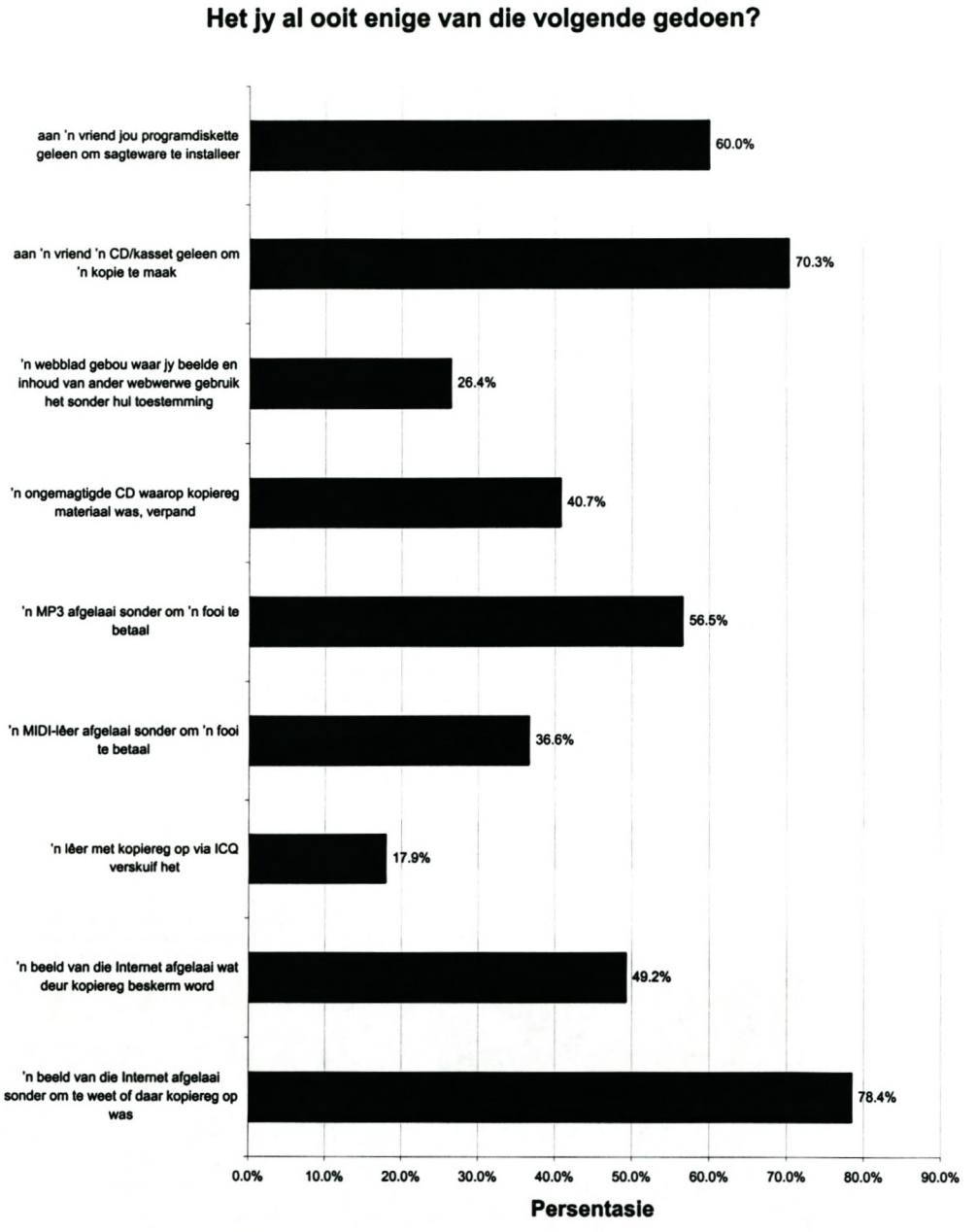


Bron: www.survey.net

Uit Tabel 5.2 is dit duidelik hoe min agting of begrip Internet-gebruikers vir kopiereg op die Internet het. Altesaam 78,4% van die Internet-gebruikers wat aan www.survey.net se opname deelgeneem het, het al 'n beeld van die Internet afgelaai sonder om te weet of daar kopiereg op was. Daar is ook 'n groot hoeveelheid Internet-gebruikers (60% en 70%) wat onderskeidelik programdiskette of CD's aan vriende leen om kopieë te maak.

Stellenbosch University http://scholar.sun.ac.za

TABEL 5.2:

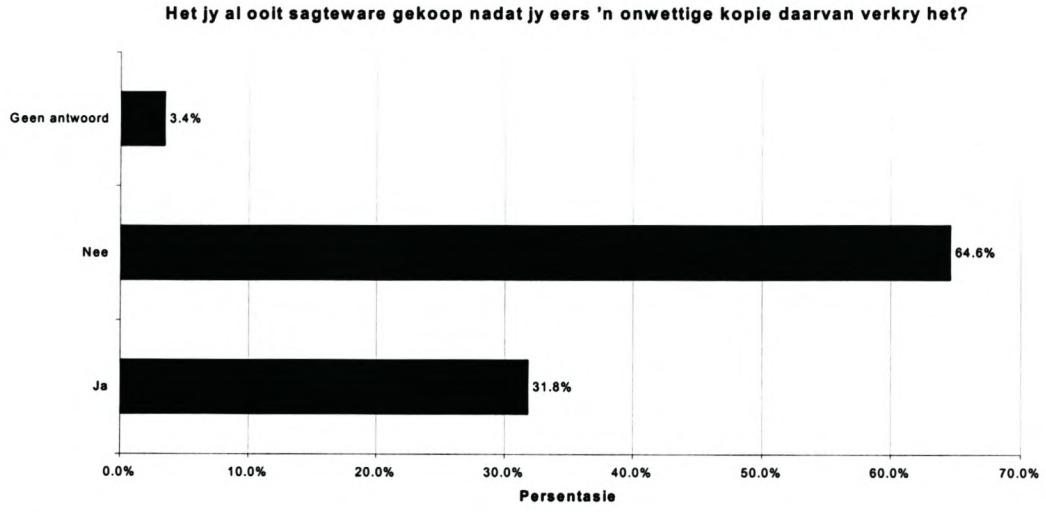


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

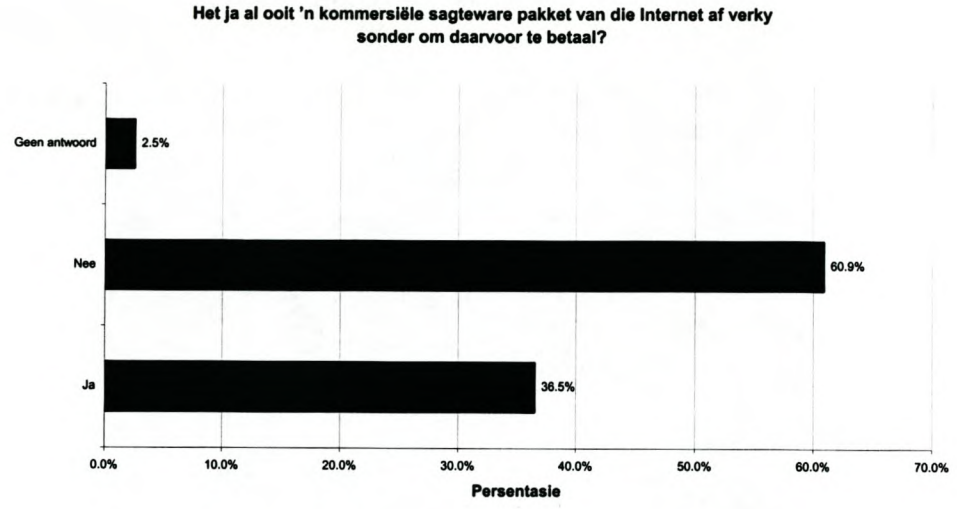
Baie Internet-gebruikers (64.6%) het al onwettige kopieë van sagteware gekry en nooit die wettige sagteware-pakket aangekoop nie (Sien Tabel 5.3). Dit stem ooreen met die 60% Internet-gebruikers wat programdiskette aan vriende uitleen, soos in Tabel 5.2 aangedui. Uit Tabel 5.4 is dit duidelik dat die Internet se sekuriteit goed is, aangesien 60% van die Internet-gebruikers wat aan die opname deelgeneem het, aangedui het dat hulle nooit 'n kommersiële sagteware pakket van die Internet kon aflaai sonder om daarvoor te betaal nie.

TABEL 5.3:



Bron: www.survey.net

TABEL 5.4:

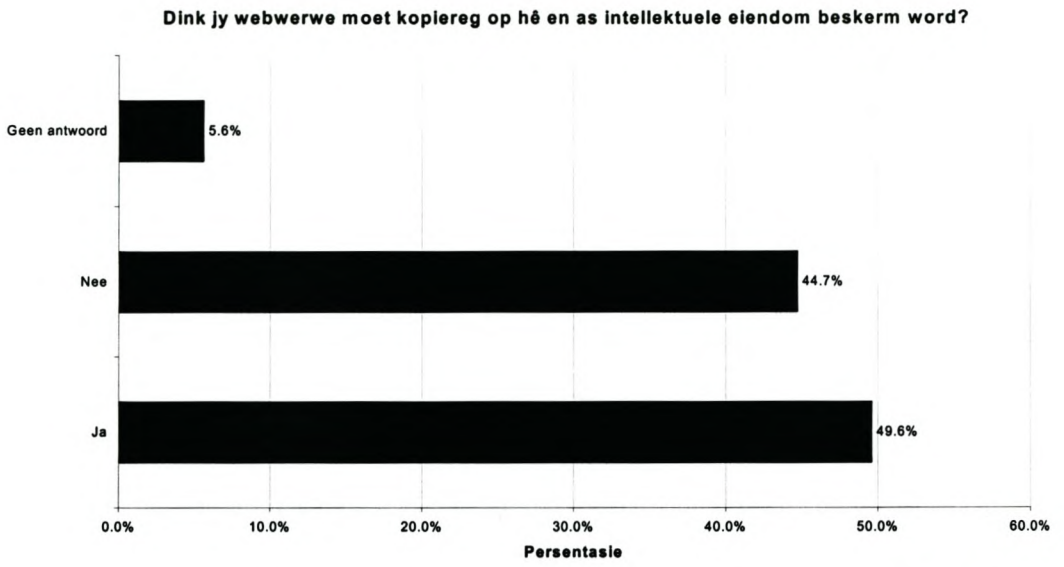


Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Altesame 49.6% van die Internet-gebruikers het in die opname aangedui (sien Tabel 5.5) dat hulle dink webwerwe moet kopiereg hê en as intellektuele eiendom beskerm word. Dis egter kommerwekkend om te sien dat 44.7% aangedui het dat dit nie nodig is nie.

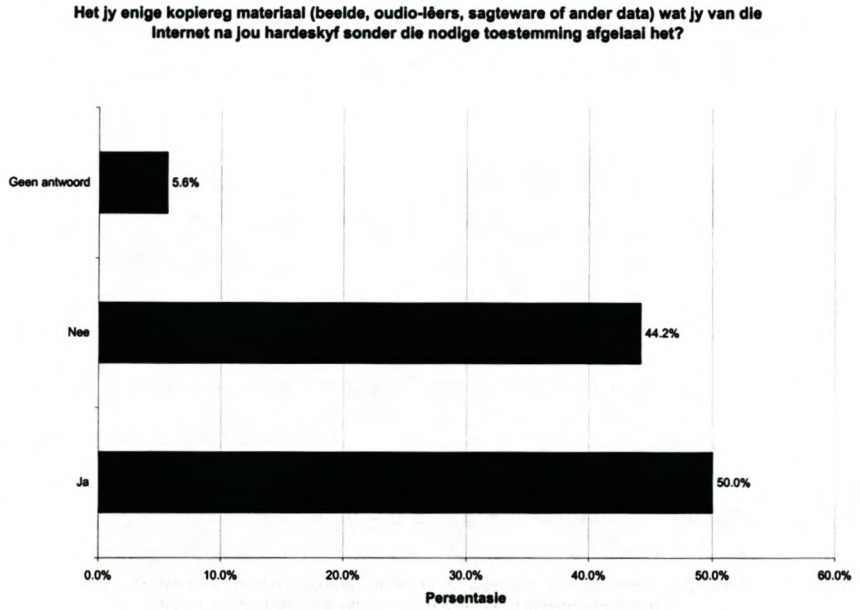
TABEL 5.5:



Bron: www.survey.net

In die opname van www.survey.net het 50% van die deelnemers aangedui hulle het materiaal op hul hardeskyf wat eintlik deur kopiereg beskerm word, wat hulle afgelaai het sonder om die nodige toestemming te kry (sien Tabel 5.6).

TABEL 5.6:



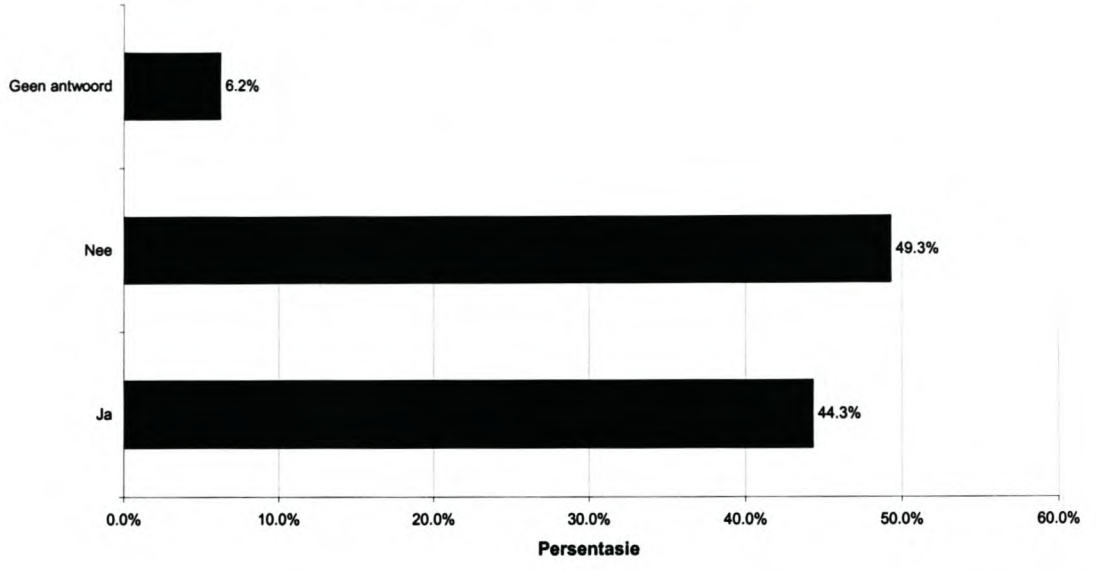
Bron: www.survey.net

Stellenbosch University http://scholar.sun.ac.za

Daar was egter minder Internet-gebruikers wat aan die opname deelgeneem het wat kopiereg-materiaal op hul rekenaar geïnstalleer het (sien Tabel 5.7).

TABEL 5.7:

Het jy enige kopiereg-materiaal (beelde, audio-lêers, sagteware of ander data) wat op jy rekenaar geïnstalleer het, sonder die nodige lisensie?



Bron: www.survey.net

5.5 Handelsmerke en domeinname

Dit is vanselfsprekend dat die reg van eienaarskap op 'n domeinnaam, wat dieselfde is as die handelsmerk of 'n gedeelte van die handelsmerk, belangrik vir enige onderneming sou wees sedert die Internet so 'n belangrike bemarkingsgereedskap geword het. 'n Domeinnaam is 'n bate vir enige onderneming. In die laaste paar jaar het daar verskeie dispute ontstaan tussen diegene wat geen wetlike aanspraak op 'n domeinnaam het nie en die ware handelsmerkhouers wat wetlik daarop aanspraak kan maak om die domeinnaam in hulle naam te registreer (Viljoen, Du Plessis & Vivier, 2001: 74).

'n Handelsmerk is enige teken wat gebruik of bedoel word om te gebruik deur 'n persoon met betrekking tot goedere en dienste met die doel om dié persoon se goedere en dienste van ander te onderskei.

Handelsmerke kan breedweg verdeel word in geregistreerde handelsmerke en ongeregistreerde handelsmerke. Om 'n handelsmerk te registreer, is nie verpligtend nie, maar handelsmerkregistrasie voorsien die houer daarvan van 'n sterk statutêre beskerming en los oortredings op (Viljoen, Du Plessis & Vivier, 2001: 71).

Stellenbosch University http://scholar.sun.ac.za

Die verskil tussen geregistreerde en ongeregistreerde handelsmerke in Suid-Afrika sal in Hoofstuk 6 bespreek word.

In die "aflyn" wêreld verteenwoordig ondernemings se handelsmerke hul identiteit in die mark, dit maak hulle en hul produkte herkenbaar vir die persone en entiteite met wie hulle handel, veral hul kliënte. In die "aanlyn" wêreld van die Internet dien domeinname dieselfde doel as 'n handelsmerk omdat 'n onderneming se teenwoordigheid op die Internet by sy domeinnaam begin (Silber, 2000:1).

Wanneer handelsmerke en domeinname bespreek word, is dit noodsaaklik om na die verskille tussen die domeinnaam en handelsmerkregistrasie te kyk, die proses van domeinnaamregistrasie, handelsmerk en domeinnaamkonflikte, die Internasionale ontwikkelings op die domeinnaamgebied en die konsep van kuberplakkery ("cybersquatting").

5.5.1 Die verskille tussen die domeinnaam- en handelsmerkregistrasie

Elke domeinnaam moet uniek wees. Met die registrasie van handelsmerke kan 'n verskeidenheid of identiese handelsmerke 'n gelyke bestaan op die handelsmerkregister voer as hulle byvoorbeeld gebruik en geregistreer is vir verskillende goedere en dienste of in verskillende gebiede geregistreer is. Van al die eienaars wat die identiese handelsmerk besit, kan slegs een die ooreenstemmende domeinnaam registreer en gebruik.

Die registrasie van enige domeinnaam wat nie presies identies is aan 'n domeinnaam wat reeds op die register is nie, word toegelaat. Dit word dus nie verbied om 'n ooreenkomstige (en soms verwarrende) domeinnaam aan verskillende eienaars in dieselfde bedryf toe te ken nie.

5.5.2 Die domeinnaamregistrasie-proses

Die registrasie van 'n domeinnaam bestaan gewoonlik uit 'n vorm wat op elk van die administratiewe webwerwe van die verskillende domeine beskikbaar is. Die vorm word dan ge-e-pos, gefaks of met die hand afgelewer na die administrateur van die betrokke domein.

Die volgende inligting word gewoonlik deur die domein-administrateurs verlang:

1. Die volle domeinnaam wat geregistreer moet word
2. Die onderneming/organisasie in wie se naam die domeinnaam geregistreer gaan word
3. 'n Administratiewe en tegniese kontak
4. 'n *Domicilium citandi et executandi* (Viljoen, Du Plessis & Vivier, 2001: 75).

Stellenbosch University http://scholar.sun.ac.za

5.5.3 Handelsmerk- en domeinnaam-konflikte

Domeinnaamregistrateurs het oor die algemeen 'n passiewe ingesteldheid ingeneem en domeinname word op 'n eerste-hier-eerste-bedien basis toegeken. Die bepalings en voorwaardes van die registrasie stel dit gewoonlik dat die administrateurs nie die hulpbronne het of wetlik verplig word om domeinname te keur vir derdeparty-oortreding nie. Daarom gebeur dit dat 'n persoon 'n domeinnaam registreer waarop hy geen reg het nie (Viljoen, Du Plessis & Vivier, 2001: 74).

In sommige gevalle is daar in die bepalings en voorwaardes voorsorg getref wat die registrasie reguleer sodat 'n domeinnaam hertoegewys kan word indien dit vir 'n tydperk van 90 dae of langer nie gebruik is nie. In die praktyk word die hertoewysing van domeinname selde toegepas.

Dit is gewoonlik onvoldoende vir die domeinnaam-eienaar om op skrif aan die handelsmerk-eienaar te stel dat hy die domeinnaam-registrasie prysgegee het nie. Die domeinnaam-registrateur verwag dat die domeinnaam-eienaar die administrateur per e-pos of brief in kennis stel dat hy bereid is om die domeinnaam prys te gee. Slegs dan sal die administrateur bereid wees om die betrokke domeinnaam aan sy ware eienaar (die handelsmerk-eienaar) toe te deel.

Dit gebeur ook dikwels dat die domeinnaam-eienaar nie sy regstrasiegelde betaal het nie. Domeinnaam-registrateurs verwag dat die domeinnaam-eienaar binne 90 dae vandat die registrasie van 'n domeinnaam goedgekeur is die registrasiegelde betaal. Dit veroorsaak dat die domeinnaam na die 90 dae tydperk heeltemal geskrap word. Die handelsmerk-eienaar het die opsie om te wag dat die domeinnaam geskrap word, waarna die domeinnaam in die handelsmerk-eienaar se naam geregistreer kan word. Die nadeel hiervan is dat dit 'n paar maande duur vir die domein-administrateur om 'n domeinnaam te skrap.

Die enigste ander metode is om stappe teen handelsmerk-oortreding of teen onregverdige kompetisie te neem. Die Suid-Afrikaanse omstandighede waarvolgens domeinnaam-registrasie as 'n handelsmerk oortreding klassifiseer, sal in Hoofstuk 6 bespreek word (Viljoen, Du Plessis & Vivier, 2001: 74-76).

■ Handelsmerke as Internet-soekterme

Die meeste webblaaie op die Wêreldwye Web bevat verskuilde sleutelwoorde en frases wat "metamerkers" ("metatags") genoem word. Die metamerkers word deur soek-enjins gebruik om inhoud op die Internet te kry. Wanneer 'n Internet-gebruiker 'n soektog deur middel van een van die menigte soek-enjins gebruik, soek die soek-enjin vir pare tussen die soekterm en die metamerkers van miljoene webwerwe. As die soekterm ooreenstem met 'n webwerf se metamerker, word die webwerf as 'n trefresultaat ("hit") in die soekresultate gelys.

Stellenbosch University http://scholar.sun.ac.za

Sonder metamerker-indeksering sal dit vir gebruikers en bemarkers moeilik wees om op die Internet te kry waarna hulle soek. Vir diegene wat Internet-bemarking doen, kan die feit dat jou webwerf as 'n trefresultaat gelys word, die verskil beteken tussen die ontwikkeling van handelsmerk-lojaliteit en om jou kliënte aan 'n direkte mededinger te verloor. Daarom is die keuse van metamerkers strategies noodsaaklik om 'n suksesvolle Internet-teenwoordigheid te verseker.

Wat gebeur egter as mededingers mekaar se handelsmerke as metamerkers in hul eie webwerwe insluit sodat 'n soektog na "Onderneming A" tot gevolg het dat "Onderneming B" as trefresultaat gelys word? In die *The Internet Law Journal* "The Legal Risks of Trademarks as Internet Search Terms" (2000) sê die skrywers sekere ondernemings doen presies dit. "Die gebruik van metamerker-tegnologie kan die misleiding van kliënte en die onredelike gebruik van mededingers se handelsmerke tot gevolg hê" (Polak, Miller & Jinnett, 2000:1).

Volgens Polak, *et al* (2000) het ondernemings begin om metamerker-gebruik deur hul mededingers te ondersoek omdat dit so belangrik is vir ondernemings om die klandisiewaarde van hul handelsmerke te beskerm. Waar nodig, het dié ondernemings 'n regsgeding teen die mededingers aanhangig gemaak om die gebruik van die metamerkers te stop. Howe het bevind dat die gebruik van 'n mededinger se handelsmerk as metamerker 'n handelsmerk-oortreding, onredelike kompetisie en vals advertering is (Polak, Miller & Jinnett, 2000:2).

5.5.4 *Internasionale ontwikkelings van domeinnaam-dispuutresolusies*

'n Aantal inisiatiewe is van stapel gestuur om die groeiende probleme rondom die toekenning en gebruik van Internet-domeinname te bekamp. Sekerlik een van die belangrikste inisiatiewe was ISOC se stigting van die IAHC (Internasionale Ad Hoc Komitee). Die komitee het elf lede gehad, insluitende verteenwoordigers van WIPO (Wêreld Intellektuele Eiendom Organisasie), INTA (Internasionale Handel Mark Vereniging) en ITU (Internasionale Telekommunikasie Unie). Die komitee het sy finale verslag in Februarie 1997 ingedien. Daarin is 'n plan aangekondig wat die volgende riglyne insluit:

1. die bekendstelling van sewe nuwe generiese top-struktuur domeine (aanvullend tot die bestaande vyf)
    - .firm vir ondernemings, of firma's
    - .shop vir ondernemings wat goedere aanbied om te verkoop
    - .web vir entiteite wat aktiwiteite beklemtoon wat verband hou met die Wêreldwye Web
    - .arts vir entiteite wat kulturele en vermaak-aktiwiteite beklemtoon
    - .rec vir entiteite wat rekreasie en vermaak-aktiwiteite beklemtoon
    - .info vir entiteite wat inligtingsdienste verskaf
    - .nom vir individue of 'n persoonlike *nom de plume*

Stellenbosch University http://scholar.sun.ac.za

2. die skep van 'n internasionale span kenners om dispute en betwisting van domeinnaam-registrasie op te los wat deur WIPO geadministreer sal word.
3. die aanstelling van tot dertig nuwe domeinnaam-registrateurs (Viljoen, Du Plessis & Vivier, 2001: 86).

IAHC het 'n privaatsektor-raamwerk geskep wat die gTLD-MoU ("Generic Top-Level Domain Memorandum of Understanding") genoem is. Dit was die internasionale raamwerk waarbinne die administrasie en versterking van die Internet se DNS (Domeinnaam Stelsel) ontwikkel en uitgevoer is. Die beleide is ontwikkel in samewerking met IANA ("Internet Assigned Numbers Authority") wat die wortel van die DNS bestuur het.

Ingesluit by die gTLD-MoU was die bykomende top-struktuur domeine, die kies van nuwe domeinregistrateurs en die ontwikkeling van billike dispuutresolusie-meganismes. Die MoU is ontwikkel as deel van 'n DNS administrasie plan van die reeds ontbinde IAHC.

Die begin van die werklike registrasie was vir Maart 1998 beplan, maar is in Februarie 1998 uitgestel weens 'n groenskrif van die Amerikaanse regering. Dié groenskrif het baie van die gTLD-MoU raamwerk se idees geïnkorporeer, maar het ook menings bevat wat van die gTLD-MoU afgewyk het.

Daarna het die Amerikaanse Departement van Handel sy hersiene beleidsdokument oor die bestuur van die Internet se domeinnaamstelsel (die witskrif) vrygestel, waarin die VSA se beleid vir die privatisering van die domeinnaamstelsel uiteengesit word (Viljoen, Du Plessis & Vivier, 2001: 86-88).

■ ICANN se UDRP (Uniform Dispute Resolution Policy)

ICANN ("Internet Corporation for Assigned Names and Numbers") is in 1998 gestig uit die Amerikaanse Department van Handel se besluit om die tegniese administrasie van die Internet te privatiseer (Franze, 2000). Op 24 Oktober 1999 het ICANN die UDRP (Uniform Dispute Resolution Policy) aangeneem wat op 1 Desember 1999 in werking getree het (Sien Bylae A).

Die UDRP lê 'n stelsel voor waar geregistreerders van 'n domeinnaam sekere soorte dispute aan 'n verpligte administratiewe proses moet onderwerp wat deur goedgekeurde dispuutresolusie-verskaffers behartig word (Tagoe, 2000). ICANN verskaf 'n lys van die goedgekeurde verskaffers met skakels na hul webwerwe. Die volgende is goedgekeurde dispuutresolusie-verskaffers:

1. ADNDRC ("Asian Domain Name Dispute Resolution Centre"): 28 Februarie 2002 goedgekeur. ADNDRC het twee kantore, een in Beijing en een in Hong Kong, met afsonderlike aanvullende reëls vir elkeen.

Stellenbosch University http://scholar.sun.ac.za

2. CPR Institute for Dispute Resolution (CPR): 22 Mei 2000 goedgekeur. CPR se kantore is in New York.
3. eResolution (eRes): 1 Januarie 2000 goedgekeur. Die Amerikaanse dispuutresolusie-verskaffer aanvaar nie prosedures wat ná 30 November 2001 begin het nie.
4. Die Nasionale Arbitrasie Forum: 23 Desember 1999 goedgekeur. Die Nasionale Arbitrasie Forum van Amerika se kantore is Minneapolis.
5. WIPO ("World Intellectual Property Organization"): 1 Desember 1999 goedgekeur. WIPO se kantore is in Geneva, Switserland ("Approved Providers", 2002:1-3).

Die UDRP gee aan die goedgekeurde verskaffers beperkte jurisdiksie om sake waarby "misbruikte registrasies" betrokke is, aan te hoor en 'n uitspraak te lewer.

Die uitspraak van die meeste sake word beslis rondom twee faktore wat in die UDRPparagraaf 4(a)(ii) en (iii) gelys word:

1. die vermoë van die aanklaer om te wys dat die respondent geen reg om wetlike belang het in die domeinnaam nie;
2. dat die respondent kwade trou betoon het in die registrasie en gebruik van die domeinnaam (Tagoe, 2000:2).

Die regulering van nasionale domeinname verskil van land tot land. Die Verenigde Nasies se WIPO ("World Intellectual Property Organization") en domeinnaam-registrateurs het reëls vir die TLD's ("top level domains") soos .com, maar daar is geen internasionale standaarde vir die domeine wat individuele lande verteenwoordig nie.

Volgens WIPO se assistent-direkteur-generaal, Francis Gurry, kan die tekort aan internasionale reëls kuberplakkery bevorder (Lyman, 2001:1-3).

5.5.5 Kuberplakkery

Die mediamaatskappy Time Warner het die regte tot meer as 100 domeinnaam-variasies wat betrekking het op die Harry Potter boekereeks verkry deur 'n uitspraak wat die Verenigde Nasies se WIPO gelewer het. Die VN paneel het die uitgewer HarperStephens van Agoura Hills, Kalifornië, aangesê om 107 variasies van die Potter domeinnaam prys te gee. HarperStephens het die meeste van dié domeinname by Network Solutions geregistreer direk nadat Time Warner aangekondig het dat hy van plan is om 'n rolprent van die Potter trefferverkoper te maak.

Die WIPO paneel het saamgestem dat HarperStephens se registrasie van domeinname soos www.harrypottersmovie.com, www.harrypotterfilm.org en www.harrypotterinhollywood.com as kuberplakkery gesien kan word.

Stellenbosch University http://scholar.sun.ac.za

Kuberplakkery is wanneer gevestigde ondernemings en handelsname as domeinname geregistreer word met die enigste doel om dit aan dié gevestigde ondernemings en handelsname terug te verkoop (Lyman, 2001).

Die probleem met kuberplakkery is dat regulering nie goed genoeg ontwikkel is om dit voldoende te bekamp nie. Volgens WIPO moet die internasionale gemeenskap begin saamstem oor watter regulering van toepassing is as hulle die groeiende probleem van kuberplakkery wil stop.

In 2001 het WIPO 'n ondersoek gepubliseer waarin hulle tot die gevolgtrekking kom dat die huidige regulering van die Internet DNS heeltemal onvoldoende is en dat 'n breër stel reëls ontwikkel moet word. Die verbeterde regulering moenie net handelsmerke beskerm nie, maar ook persoonlike name, die name van lande en sekere ander geografiese name, name en afkortings van internasionale ondernemings en generiese name vir farmaseutiese middels. So byvoorbeeld word die domeinnaam southafrica.com deur 'n Amerikaanse onderneming besit (McDonald, 2001).

5.6 Kubermisdaad

Die berugte Amerikaanse kuberkraker en "rekenaarterroris", Kevin Mitnick, was drie jaar lank besig om van die FBI (Federal Bureau of Investigation) te vlug nadat hy deur middel van kuberkrakery toegang tot Novell Inc., Motorola Inc, Sun Microsystems Inc, Nokia Corp en die rekenaarwetenskaplike Tsutomu Shimomura, wat die regering gehelp het om hom te vang, se netwerkstelsels verkry het (Abrea, 2002). Op 20 Januarie 2003 is Mitnick vrygestel van die voorwaardes van sy toesighoudende vrylating wat hom verbied om 'n rekenaar te gebruik of om as 'n konsultant in rekenaarverwante aangeleenthede op te tree ("Free Kevin Mitnick", 2002:1).

Die Amerikaanse geheime diens het op 24 Oktober 1994 geglo hulle het Mitnick vasgetrek toe hulle 'n klopjag gedoen het op 'n woonstel in Seattle wat aan 'n "Brian Merrill" verhuur is. Al wat hulle gekonfiskeer het, was Mitnick se satelliet, die Toshiba Satellite 4400SX. Op 15 Februarie 1995 was Mitnick egter nie so gelukkig nie en is hy uiteindelik in sy woonstel in Raleigh, Noord-Carolina, gearresteer. Hy is vier en 'n half jaar aangehou sonder 'n opsie van borgtog.

In Maart 2000 het Mitnick skuldig gepleit op aanklagte van telegraaf-bedrog ("wire fraud"), rekenaarbedrog en die onderskepping van elektroniese kommunikasie. Hy is toe vrygelaat onder toesighoudende voorwaardes en bly nou naby Los Angeles waar hy besig is om 'n boek, *The Art of Deception*, te skryf. Hy is tot en met 2010 verbied om geld te maak deur sy eie storie te vertel (Abrea, 2002).

Mitnick is een van die berugste kuberkrakers wat onder Amerikaanse wetgewing vir kubermisdaad gevonnis is. Uit die kort opsomming van Mitnick se verhaal is dit duidelik dat die Internet ook 'n groot aantal misdaadprobleme skep. Rekenaarmisdadigers, soos Mitnick, het die

Stellenbosch University http://scholar.sun.ac.za

geleentheid gekry om toegang tot sensitiewe inligting te kry omdat hulle die vermoë het om dit te doen.

Rekenaarmisdaad dek 'n baie wye veld. Aan die een kant bestaan dit uit "tradisionele misdaad" wat die steel van rekenaarstelsels en hardeware behels. Aan die anderkant word rekenaarmisdaad gepleeg deur die gebruik van hoogs tegnologiese gereedskap om rekenaarstelsels te manipuleer en te infiltreer wat dalk aan die anderkant van die wêreld sit. Volgens Barrie Gordon wat die hoofstuk *Internet criminal law* in Cyberlaw@SA (2001, 423) geskryf het, kan daar na rekenaarmisdaad verwys word as enige kriminele aktiwiteit waarby 'n rekenaar betrokke is.

Rekenaarmisdaad kan in twee breë kategorieë ingedeel word:

1. kriminele aktiwiteite wat gepleeg word deur slegs 'n rekenaarstelsel te gebruik, bv. kuberkrakery en pakket snuffel (sien punt 5.5.3).
2. misdade wat al eeue lank bestaan, maar nou deur middel van 'n rekenaarstelsel gepleeg word, bv. diefstal, bedrog en kinderpornografie.

Die nuwe misdade wat hier bespreek word, is kuberkrakery, gevaarlike kodes, pakket-snuffel en gewone misdaad wat deur middel van rekenaarstelsels gepleeg word.

5.6.1 Kuberkrakery

Ongemagtigde toegang tot rekenaars word algemeen as kuberkrakery beskou. Dit beteken eenvoudig dat die indringer aanteken tot die rekenaarnetwerk en toegang verkry sonder die nodige gesag om dit te doen (Gordon, 2001: 423-425).

Kuberkrakers kan in twee kampe ingedeel word:

1. **Die "withoed"-krakers ("hackers"):** Hulle beweer hulle word gemotiveer deur die soeke na kennis en begrip van rekenaarstelsels (Dudley, 2002: 60). Oor die algemeen verkry die "withoed"-kuberkrakers toegang tot rekenaarstelsels net om te weet hoe dit werk en die "withoed" kry bevrediging daaruit net om te weet hy het die stelsel om die bos gelei. Dit gebeur bykans nooit dat 'n "withoed" 'n stelsel sal beskadig nie. Die meeste van die tyd sal die "withoed" slegs 'n "vlag"[3] in die rekenaarstelsel sit om te wys hy was daar, maar dit bly steeds 'n kriminele oortreding.
2. **Die "swarthoed"-krakers ("crackers"):** Hulle het reeds die regsgrense oorgesteek en is die meeste van die tyd verantwoordelik vir vandalisme en het slegte motiewe soos gierigheid of wraak (Dudley, 2002: 60). Hulle is die indringers wat nie net toegang tot 'n rekenaarstelsel wil kry nie, maar bybedoelings het. Hulle bring gewoonlik rekenaarstelsels tot 'n stilstand, of sal kopieë van sensitiewe inligting maak om dit op 'n onwettige manier te gebruik (Gordon, 2001: 425).

---

[3] 'n "Vlag" is gewoonlik 'n klein tekslêer waarin daar melding gemaak word dat 'n spesifieke kuberkraker daar was, bv. "Phreeak was here" (Dudley, 2002: 60).

Stellenbosch University http://scholar.sun.ac.za

Kuberkrakers praat hulle eie taal en staan altyd bekend onder kodename soos r00t3rs of seebs (Dudley, 2002: 60).

Volgens Gavin Dudley se artikel in *Finansies & Tegniek* (2002: 60) is dit bykans onmoontlik om 'n misdaadprofiel van kuberkrakers saam te stel. Clive Handley, sake-ontleder by die netwerkmaatskappy Namitech sê:

> "Dis moeilik om akkurate inligting oor krakers te kry of om 'n profiel saam te stel omdat hul bedrywighede ondergronds gehou word en hulle selde hul motief bekend maak waarom hulle 'n stelsel binnegedring het" (Dudley, 2002: 60).

Die meeste maatskappye het begin om krakers aan te stel vir nywerheidspioenasie. Sommige krakers en krakerbendes wat hulself aan die owerhede bekendgemaak het, help nou wetstoepassers en tree as sekuriteitskonsultante op (Dudley, 2002: 60).

5.6.2 Gevaarlike kodes

Gevaarlike kodes verwys na enige rekenaarprogram wat die uitwissing of beskadiging van 'n rekenaarstelsel tot gevolg het. Die kodes word in verskillende vorms aangetref, soos virusse, Trojaanse perde en wurms.

Gevaarlike kodes kan ook verwys na rekenaar-toepassings wat nie voldoende ontfout is nie. In so 'n geval sal die rekenaar ook wanfunksioneer (Gordon, 2001: 426).

■ Virus

'n Virus is 'n bekende vorm van 'n gevaarlike kode. Dit is 'n klein rekenaarprogram wat homself aan 'n rekenaartoepassing of ander lêer heg en homself op die gebruiker se stelsel kopieer. Dit reproduseer homself om soveel as moontlik van die gasheer-rekenaar se lêers te besmet totdat die rekenaar wanfunksioneer. As 'n besmette lêer op 'n ander rekenaar gekopieer word, sal daardie rekenaar ook besmet word (Gordon, 2001: 426).

■ Trojaanse perd

Soos in die mite van die Trojaanse perd, besmet dié kode van binne. 'n Kuberkraker sal gewoonlik 'n Trojaanse perd-lêer op 'n gasheer-rekenaar kopieer en dit vermom sodat dit baie soos 'n normale toepassing lyk. Wanneer die gemagtigde gebruiker die toepassings in werking stel omdat hy dink dit is 'n gewone toepassing, sal die Trojaanse perd die rekenaarstelsel beskadig. 'n Trojaanse perd kan ook geprogrammeer word om sensitiewe inligting, soos veranderings van gebruikers se wagwoorde, aan die kuberkraker te stuur (Gordon, 2001: 427).

Stellenbosch University http://scholar.sun.ac.za

- **Wurm**

'n Wurm is 'n klein, onafhanklike rekenaarprogram wat homself in 'n rekenaarstelsel wegsteek. Wurms heg hulself nie aan toepassingslêers soos virusse nie, maar kruip in die stelsel weg. Wanneer 'n sekere gebeurtenis plaasvind, (soos 'n verandering in datum) word die wurm aan die gang gesit (Gordon, 2001: 427).

5.6.3 Pakket-snuffel

Wanneer inligting oor die Internet gestuur word, word die boodskap in kleiner dele opgedeel, wat data-pakkette genoem word. Dié pakkette word een vir een oor die Internet na die ontvanger gestuur en die ontvanger se rekenaar plaas die pakkette in die regte volgorde en kombineer hulle weer om die een boodskap te vorm wat die ontvanger dan lees.

Wanneer die pakkette oor die Internet reis, kan hulle maklik onderskep word en 'n kopie van die oorspronklike pakket kan gemaak word. Dit staan bekend as pakket-snuffel. Die indringer kan die pakkette lees en sodoende waardevolle inligting bekom, soos kredietkaartinligting, bankstate of ander geklassifiseerde inligting (Buys, 2001: 428-429).

5.6.4 Gewone misdaad

Dit is bestaande misdade wat nou deur middel van die Internet gepleeg word. Voorbeelde is:

1. **Internetbedrog:** Dit kan op 'n verskeidenheid maniere plaasvind. Daar is so baie Internetbedrog wat elke dag op die Internet plaasvind, dat sekere webwerwe se primêre doel is om oor die jongstes verslag te doen. Die algemene wetgewing wat betrekking het op bedrog het ook op Internetbedrog betrekking (Gordon, 2001: 430).
2. **Inligtingsdiefstal:** 'n Voorbeeld van inligtingsdiefstal is identiteitsdiefstal. Dit is wanneer iemand se persoonlike besonderhede deur 'n ander persoon gebruik word, soos kredietkaartnommers, idenditeitsnommer en 'n persoon se naam (Gordon, 2001: 432).
3. **Kopieregskending:** reeds onder punt 5.3 bespreek.
4. **Internet-dobbelary:** Sedert die begin van die Wêreldwye Web was dit maklik om aanlyn dobbelary aan die wêreld bekend te stel. Dobbelaars plaas hul weddenskappe oor die Internet en binne sekondes kan hulle uitvind of hulle gewen het of nie. As hulle gewen het, word daar dadelik 'n elektroniese betaling aan hulle gemaak (Gordon, 2001: 436).
5. **Kinderpornografie:** Wanneer 'n persoon 'n publikasie of 'n film skep, vervaardig, invoer of besit wat kinderpornografie bevat, sal die persoon aan 'n kinderpornografie-misdaad skuldig wees (Gordon, 2001: 439).

Stellenbosch University http://scholar.sun.ac.za

5.6.5 *Jurisdiksieprobleme in die kuberruim*

Die probleem met jurisdiksie in die kuberruim hou verband met die Internet se bykans grenslose omstandighede. Die grense wat wel in die Internet bestaan, verskil totaal en al van die grense wat ons in die "regte" wêreld aantref.

Sommige bedieners en webwerwe vereis wagwoorde voordat 'n gebruiker toegang kry. As die gebruiker nie die regte wagwoord het nie, kan hy nie toegang kry nie. Dié soort webwerwe is in die minderheid. Die grootste deel van die Internet is beskikbaar vir alle Internet-gebruikers, maak nie saak waar hulle is nie. Die konsep van jurisdiksie soos dit tans bekend is, hou verband met soewereine state en hul uitgemerkte grense. Die Internet verontagsaam die grense heeltemal.

'n Gebruiker kan toegang tot tientalle webwerwe in net soveel verskillende lande in 'n kwessie van minute kry sonder om eens te weet waarvandaan die inligting afkomstig is. Die probleem raak egter erger wanneer 'n misdadiger in een land 'n Internet-verwante oortreding in 'n ander land begaan. Op die oomblik kan 'n misdadiger net onder die land waarin die oortreding plaasgevind het, se jurisdiksie geplaas word as hy aan die land uitgelewer word.

Uitlewering is wanneer 'n beskuldige of 'n gevonnisde individu aan die land waarin hy beskuldig word, of gevonnis is, oorhandig word deur die staat binne wie se grense hy op daardie stadium is.

Die proses van uitlewering is 'n sensitiewe politieke saak en word slegs vir die ergste oortredings oorweeg (Gordon, 2001: 441-442).

5.6.6 *Internasionale ontwikkelinge*

Die Europese Raad het sedert 1997 aan sy internasionale Konvensie oor Kubermisdaad gewerk. Op 23 November 2001 het 26 van die lidlande die konvensie in Boedapest onderteken. Kanada, Japan, Suid-Afrika en die VSA was ook by die opstel van die konvensie betrokke ("The draft international Convention", 2001:1).

Dié Konvensie (Sien Bylae B) is die eerste internasionale ooreenkoms oor misdade wat via die Internet en ander rekenaarnetwerke gepleeg word. Dit het veral te make met die oortreding van kopiereg, rekenaarverwante bedrog, kinderpornografie en oortredings van netwerk-sekuriteit. Dit bevat ook 'n reeks kragte en prosedures soos die ondersoek van rekenaarnetwerke en onderskepping.

Die hoofdoel van die konvensie, soos in die voorwoord uiteengesit word, is om 'n algemene misdaadvoorkomingsbeleid na te streef wat daarop gemik is om die gemeenskap teen

Stellenbosch University http://scholar.sun.ac.za

kubermisdaad te beskerm deur veral geskikte wetgewing aan te neem en internasionale samewerking aan te moedig.

Die Konvensie sal ook aangevul word deur 'n Addisionele Protokol wat enige publikasie van rassistiese of xenofobiese propaganda via 'n rekenaarnetwerk 'n kriminele oortreding maak ("Convention on Cybercrime", 2001:16-23).

5.7 Samevatting

Die hardeware wat die ruggraat van die Internet vorm, moet êrens in die fisieke wêreld geïnstalleer wees. Op die oomblik bestaan die ruggraat van die Internet uit verskeie rekenaars met modems en bedieners regoor die wêreld, fisieke telefoonkabels, aardsversenders en satelliete (Alberts, 2001: 395).

Die regulering van die fisieke komponente van die Internet is tot 'n mate as gevolg van sy fisieke teenwoordigheid deur blote toeval, gereguleer. Dit is omdat die ruggraat nie oorspronklik vir die Internet geskep is nie, maar vir die telefoon. Regerings het seker gemaak toe hulle telefoon-kommunikasie toegelaat het, dat daar voldoende regulering binne hul landsgrense daarvoor was. Al die lande wat van telefoon-kommunikasie gebruik gemaak het, het 'n internasionale regstelsel geskep om die skepping en implementering van universele en eenvormige standaarde regoor die wêreld te fasiliteer wat vandag bekend staan as telekommunikasie. Dit is alles moontlik gemaak deur die stigting van die Internasionale Telekommunikasie Unie wat 'n amptelike unie van die Verenigde Nasies is (Alberts, 2001: 396).

Die kern van die Internet se infrastruktuur bestaan uit roeteerders, gashere en "pype". Gashere en roeteerders word deur onder meer regeringsorganisasies, private organisasies of individue besit, terwyl "pype" meestal deur telekommunikasie-ondernemings besit word (Buys, 2001: 19).

Die fisieke verbinding tussen toegangsverskaffers stel die Internet-verkeer in staat om deur eweknie-punte te beweeg. Eweknie-ooreenkomste tussen toegangsverskaffers en Internetdiens-verskaffers, reguleer die wisseling van inligting tussen die deelnemende partye se netwerke. Dié ooreenkomste behels gewoonlik dat nie een van die deelnemers die gebruik van die inligting op hul netwerk mag beperk nie of inligting filtreer voor die versending of ontvangs nie (Buys, 2001: 21-22).

Daar bestaan verskeie wetgewende Internet-organisasies wat onder meer verantwoordelik is vir die tegniese standaarde van die Internet, dispuutresolusie en wat oor die algemeen aan die belange van die Internet-gemeenskap wil voldoen.

Die W3C (Word Wide Web Consortium) ontwikkel spesifikasies, riglyne, sagteware en gereedskappe om die www tot sy volle potensiaal te lei ("Leading the Web", 2002:1). ISOC (The

Stellenbosch University http://scholar.sun.ac.za

Internet Society) dien as 'n internasionale organisasie vir globale kommunikasie en samewerking op die Internet. ISOC bevorder 'n wye reeks aktiwiteite wat op die Internet se ontwikkeling en beskikbaarheid en soortgelyke tegnologieë gefokus is (Buys, 2001: 28). ICANN (The Internet Corporation of Assigned Names and Numbers) neem verantwoordelikheid vir 'n stel funksies wat voorheen deur die Amerikaanse regering se kontrak met IANA (Internet Assigned Numbers Authority) en ander groepe uitgevoer is. ICANN is spesifiek verantwoordelik vir die koördinering van die volgende identifiseerders wat wêreldwyd uniek moet wees vir die Internet om doeltreffend te kan funksioneer: domeinname, IP-adresnommers en protokol-parameter en poortnommers ("The Internet Corporation for Assigned Names and Numbers", 2002:1). Die VSA se Nasionale Arbitrasie Forum is een vir die vernaamste Internet domeinnaam-dispuutresolusieverskaffers in die wêreld. Dié forum verskaf oplossings deur middel van ICANN se UDRP (Uniforum Domain Name Dispute Resolution Policy).

'n Internet-gebruiker wat iets op die Internet publiseer, kan enige plek in die wêreld wette oortree. Elke land het sy eie wette wat kopiereg, handelsmerke, patente, ontwerpe en handelsname reguleer. Die aard van die Internet se grenslose omgewing sal lande dwing om wetgewing te standaardiseer.

In Suid-Afrika word internasionale verhoudings in die intellektuele eindomsveld op die oomblik deur verskeie internasionale konvensies en ooreenkomste gereguleer. Die ooreenkomste maak sommige regulering van die oortreding van intellektuele eiendomsreg oor grense moontlik deur die ondergetekendes te dwing om buitelandse werke deur die wysiging van hul plaaslike wetgewing te beskerm.

Kopiereghouers moet vanselfsprekend, wanneer hulle hul werk op 'n webwerf plaas, 'n nie-eksklusiewe lisensie aan alle Internet-gebruikers wat toegang tot die materiaal het, toestaan sodat kortstondige kopieë van die materiaal op hul rekenaars gemaak kan word. Internet-gebruikers se rekenaars wat toegang tot die webblad kry, maak 'n kopie van die materiaal op sy RAM, sodat die inhoud op sy rekenaarskerm kan verskyn (Buys, 2001: 37-38).

Die meeste kenners glo tegnologie self is die beste manier om kopiereg op die Internet te beskerm (Buys, 2001: 39). Dit is egter nie 'n voldoende reguleringsmeganisme nie, aangesien kuberkrakers daarvoor bekend is om deur die sekuriteitsmeganismes van dié tipe sagteware te breek.

Die wyse waarop die Internet werk en die grenslose samestelling van die Internet skep verskillende probleemareas vir kopiereg op die Internet.

Die hiperskakelstelsel wat grootliks die fondament van die Internet se inhoud vorm, skep veral 'n probleem wanneer inskakels ter sprake is. Inskakels maak 'n kopie van die inhoud van die

Stellenbosch University http://scholar.sun.ac.za

webblad waarna dit skakel op die webwerf waarop die skakel is. Sodoende vorm dit deel van die webwerf waarop die skakel is, sonder dat die URL verander. Raamstelsels, waar een webwerf as deel van 'n ander geïnkorporeer word, word deur inskakels moontlik gemaak. Dit is definitief 'n oortreding van kopiereg, maar alle webwerf-eienaars het een gemeenskaplike doel voor oë en dit is om te verseker dat die maksimum aantal gebruikers hul webwerwe gebruik.

Dit is egter nie 'n voldoende verweer teen inskakels nie, maar wel vir uitskakels waar die Internet-gebruiker die webwerf waarop die skakel is, verlaat en na die webwerf waarna geskakel word, gaan. Die voortbestaan van die Internet berus op webwerwe wat na ander webwerwe deur middel van uitskakels kan skakel, sonder die nodige toestemming.

Die proses van voorlopige berging is altyd 'n potensiële oortreding van kopiereg, omdat daar altyd kopieë gemaak word. Daar word egter algemeen aanvaar dat die proses van voorlopige berging noodsaaklik is vir die doeltreffende gebruik van die Internet.

In 'n aanlyn intellektuele eiendom-opname wat deur Survey.net in Mei 2002 gedoen is, het die meeste van die 1 807 Internet-gebruikers wat aan die opname deelgeneem het, al kopiereg op die Internet oortree. Dit kan aan twee faktore toegeskryf word, onvoldoende regulering van kopiereg op die Internet en onvoldoende tegnologiese sekerheidsmeganismes om kopiereg op die Internet te beskerm.

Dit is vir enige onderneming belangrik om dieselfde domeinnaam as hul handelsmerk te besit, veral vandat die Internet so 'n belangrike bemarkingsgereedskap geword het. Verskeie dispute het tussen diegene wat geen aanspraak op 'n domeinnaam het nie en die handelsmerkhouers wat wetlik daarop aanspraak kan maak, ontstaan (Viljoen, Du Plessis & Vivier, 2001: 71).

Elke domeinnaam moet uniek wees, terwyl daar 'n verskeidenheid identiese handelsmerke 'n gelyke bestaan kan voer as hulle gebruik en geregistreer is vir verskillende goedere en dienste of in verskillende gebiede. Van al die eienaars wat dieselfde handelsmerk besit, kan slegs een die ooreenstemmende domeinnaam registreer en gebruik.

Hier is die Internet se gebrek aan geografiese grense weer eens een van die hoofoorsake van die probleem. 'n Moontlike oplossing sal wees om die handelsmerkregistrasie-proses aan te pas, sodat identiese handelsmerke verbied word. Dit is egter nie prakties nie, aangesien dit groot handelsmerkdispute tot gevolg sal hê en die onkostes aan so 'n proses te groot is.

Dit word egter nog meer ingewikkeld aangesien die registrasie van enige domeinnaam wat nie presies identies aan 'n domeinnaam is wat reeds geregistreer is nie, wel toegelaat word. Daar is dus geen verbod om ooreenkomstige en soms verwarrende domeinname aan verskillende eienaars in dieselfde bedryf toe te ken nie (Viljoen, Du Plessis & Vivier, 2001: 74).

Stellenbosch University http://scholar.sun.ac.za

Domeinnaamregistrateurs se passiewe ingesteldheid teenoor die registrasie van domeinname en die eerste-hier-eerste-bedien basis waarop domeinname toegeken word, is kommerwekkend. Die bepalings en voorwaardes van die registrasie stel gewoonlik dat die administrateurs nie die hulpbronne het of wetlik verplig word om domeinname te keur vir derdeparty-oortredings nie (Buys, 2001: 74).

'n Aantal inisiatiewe is van stapel gestuur om die groeiende probleme rondom die toekenning en gebruik van Internet-domeinname te bekamp. ISOC se stigting van die IAHC (Internasionale Ad Hoc Komitee) is sekerlik een van die belangrikste inisiatiewe. IAHC het die privaatsektor-raamwerk gTLD-MoU ("Generic Top-Level Domain Memorandum of Understanding") geskep. Dit was die internasionale raamwerk waarbinne die administrasie en versterking van die Internet se DNS (Domeinnaam Stelsel) ontwikkel en uitgevoer is.

ICANN se UDRP ("Uniform Dispute Resolution Policy") lê 'n stelsel voor waar domeinnaam-eienaars sekere soorte dispute aan 'n verpligte administratiewe proses moet onderwerp, wat deur goedgekeurde dispuutresolusie-verskaffers behartig word. Die uitspraak van die meeste sake word rondom twee faktore beslis: die vermoë van die aanklaer om te bewys dat die respondent geen reg of wetlike belang het in die domeinnaam nie, en dat die respondent kwade trou betoon het in die registrasie en gebruik van die domeinnaam (Tagoe, 2000).

Die regulering van nasionale domeinname, soos .za, verskil van land tot land. Die Verenigde Nasies se WIPO en domeinnaam-registrateurs het reëls vir die TLD's ("top level domains"), maar daar is geen internasionale standaarde vir die domeine wat individuele lande verteenwoordig nie (Lyman, 2001).

Die tekort aan internasionale reëls kan kuberplakkery bevorder (Lyman, 2001). Volgens WIPO moet die internasionale gemeenskap begin saamstem oor watter regulering van toepassing is as hulle die groeiende probleem van kuberplakkery wil bekamp.

Ná 'n ondersoek in 2001 het WIPO tot die gevolgtrekking gekom dat die huidige regulering van die Internet DNS heeltemal onvoldoende is en dat 'n breër stel reëls ontwikkel moet word. Die verbeterde regulering moenie net handelsmerke beskerm nie, maar ook persoonlike name, die name van lande en sekere ander geografiese name, name en afkortings van internasionale ondernemings en generiese name vir farmaseutiese middels (McDonald, 2001).

Nuwe misdade het met die ontstaan van die Internet tot stand gekom en sluit onder meer in: kriminele aktiwiteit wat gepleeg word deur slegs 'n rekenaarstelsel te gebruik, soos kuberkrakery en pakket snuffel; en misdade wat al eeue lank bestaan maar nou deur middel van 'n rekenaarstelsel gepleeg word, soos diefstal, bedrog en kinderpornografie (Gordon, 2001: 423-424).

Stellenbosch University http://scholar.sun.ac.za

Die probleem met jurisdiksie in die kuberruim hou weereens verband met die Internet se grenslose omstandighede. Die grense wat wel in die Internet bestaan, verskil totaal en al van die grense wat ons in die "regte" wêreld aantref. 'n Gebruiker kan toegang tot webwerwe in ander lande kry sonder om eens bewus te wees waarvandaan die inligting kom. Die probleem raak egter erger wanneer 'n misdadiger in een land 'n Internet-verwante oortreding in 'n ander land begaan. Op die oomblik kan die misdadigers slegs onder die land waarin die oortreding plaasgevind het, se jurisdiksie geplaas word, as hy aan dié land uitgelewer word (Gordon, 2001: 441.442).

Die Europese Raad se internasionale Konvensie oor Kubermisdaad is die eerste internasionale ooreenkoms oor misdade wat via die Internet en ander rekenaarnetwerke gepleeg word. Die hoofdoel van die konvensie is om 'n algemene misdaadvoorkomingsbeleid na te streef wat daarop gemik is om die gemeenskap teen kubermisdaad te beskerm deur veral internasionale samewerking aan te moedig ("Conventions on Cybercrime", 2001:15).

In die volgende hoofstuk word Internet-regulering in Suid-Afrika bespreek. Die fokus van die hoofstuk val veral op Suid-Afrika se Elektroniese Kommunikasies en Transaksies Wet van 2002. Die Suid-Afrikaanse regulering van kopiereg, handelsmerke en domeinname en kubermisdaad word ook in die volgende hoofstuk bespreek.

Stellenbosch University http://scholar.sun.ac.za

HOOFSTUK 6
INTERNET-REGULERING IN SUID-AFRIKA

Die Internet in Suid-Afrika het 'n nuwe tydperk ingegaan met die Elektroniese Kommunikasie en Transaksies Wet van 2002 en die gepaargaande nasionale e-strategie. Volgens Suid-Afrika se Minister van Kommunikasie, dr. Ivy Matsepe-Casaburri, word 2002 gekenmerk deur die gebruik van elektroniese kommunikasies en transaksies van alle agtergronde ("Nuwe era ingelui", 2002: 2).

In die tydperk voor die Elektroniese Kommunikasie en Transaksies Wet van 2002 was die grootste probleemarea die regulering van die inhoud van die Internet in Suid-Afrika. Om die ruggraat van die Internet te reguleer, is relatief maklik, omdat dit die fisieke deel van die Internet vorm en daar reeds bestaande wetgewing is wat op die Internet toegepas kon word (Alberts, 2001: 414).

In dié hoofstuk word die regulering van die fisieke komponent van die Internet in Suid-Afrika, die verskillende Internet-rolspelers en -organisasies in Suid-Afrika bespreek. Die nuwe Elektroniese Kommunikasie en Transaksies Wet van 2002 word oorsigtelik bespreek. Wanneer kopiereg, domeinname en handelsmerke en kubermisdaad bespreek word, word daar na spesifieke gevallestudies verwys.

6.1 Regulering van die Internet-ruggraat in Suid-Afrika

Dit is belangrik om te weet dat die fisieke infrastruktuur van die Internet nie net in Suid-Afrikaanse grondgebied gevestig is nie, maar ook oor ander nasionale jurisdiksie en internasionale gebiede versprei is.

Dit beteken dat die Suid-Afrikaanse regstelsel slegs van toepassing sal wees op dié dele van die Internet-ruggraat wat binne die Suid-Afrikaanse landsgrense val. Wanneer dit die Suid-Afrikaanse grense oorsteek, sal een van twee jurisdiksies van toepassing raak: die jusisdiksie van 'n ander land, of die jurisdiksie van internasionale wetgewing. Dié jurisdiksies sal as volg toegepas word:

1. As die ruggraat die Suid-Afrikaanse grense horisontaal oor die oppervlak van die planeet oorsteek, is die wetgewing wat van toepassing is die ander land se wet as die ruggraat voortgaan in die gebied of in enige ander land aangrensend of naby Suid-Afrika voordat dit enige internasionale gebiede oorgesteek het. Internasionale wetgewing sal van toepassing wees as die ruggraat voortgaan in enige gebied wat nie aan enige land behoort nie, soos internasionale seewaters.

Stellenbosch University http://scholar.sun.ac.za

2. As die ruggraat die Suid-Afrikaanse grense vertikaal buite die atmosfeer van die planeet deur middel van satelliet-transmissie oorsteek, sal internasionale- en buitenste ruim wetgewing van toepassing wees (Alberts, 2001: 398).

Die regulering van die tegnologiese infrastruktuur word gedoen deur die ruggraat in twee kategorieë te verdeel:

1. telekommunikasie-gebruik, bv. telefoondienste en elektroniese data-oordrag dienste
2. uitsaai van televisie en radio (Alberts, 2001: 398).

Wanneer daar vasgestel is dat die toepassende jurisdiksie wel binne die omvang van Suid-Afrika se landsgebied val, word dit belangrik om te kyk watter Suid-Afrikaanse telekommunikasie- en uitsaai-wetgewing van toepassing is om die Internet as 'n vorm van media te reguleer.

Die Suid-Afrikaanse telekommunikasie-regime word deur die volgende statutêre dokumente/middels en beleidsriglyne gereguleer:

1. **Die Grondwet (Wet 108 van 1996):** Die Grondwet vorm die basis van die wetlike staat en verskans sekere regte wat die effektiewe implementering van beginsels wat in die Telekommunikasie-wet en beleidsraamwerk vervat is, waarborg (Alberts, 2001: 398).
2. **Die Witskrif oor Telekommunikasie:** Dit was die voorloper van die Telekommunikasie Wet 103 van 1996. Dit is steeds van toepassing omdat dit riglyne skep waarvolgens die Departement Kommunikasie beleidsriglyne vir die Suid-Afrikaanse telekommunikasiebedryf saamstel (Alberts, 2001: 399).
3. **Telekommunikasie Wet 103 van 1996:** Dié wet dek 'n wye veld in telekommunikasie, maar in wese voorsien die Wet die volgende:
   - 3.1 die regulering van telekommunikasie-bedrywighede wat nie as uitsaai-kommunikasie geklassifiseer kan word nie.
   - 3.2 beheer van die radio-frekwensie-spektrum
   - 3.3 vir die bogenoemde doel, die skep van die onafhanklike SATRA (South African Tele-communikcation Regulatory Authority) en die Universal Service Agency
   - 3.4 breë regulering van telekommunikasie-dienste in Suid-Afrika in belang van die publiek, 'n verpligting wat aan SATRA toegeken is, ingevolge seksie 2 van die Wet
   - 3.5 voorsien Telkom, die staat se telekommunikasie-diensverskaffer, van 'n vyf-jaar eksklusiewe PSTN (Public Switched Telephone Network) lisensie
   - 3.6 voorsien Vodacom (Pty) Ltd en Mobile Telephone Networks (Pty) van sellulêre telekommunikasie-dienste
   - 3.8 lisensies vir VANS (Value-Added Network Services) wat dienste insluit wat gebaseer is op die bestaande telekommunikasie-infrastruktuur van Telkom (Alberts, 2001: 400).
4. **Die Beleid op Suid-Afrikaanse Nasionale Inligtings- en Kommunikasie-hoofweg:** Op 4 Maart 1998 het die Kabinet sekere aanbevelings met betrekking tot Suid-Afrika se Nasionale Inligtings en Kommunikasie Hoofweg gepubliseer (Alberts, 2001: 407).

Stellenbosch University http://scholar.sun.ac.za

Solank as wat IDV's vir 'n VANS lisensie moet aansoek doen in terme van die Telekommunikasie-wet vir die toegevoegde waarde diens wat hulle lewer kan die fisieke komponent van die Internet in Suid-Afrika gereguleer word. Dit is die geval, hetsy die Internet-verbinding verskaf word deur middel van landlyne, landsversendings, satellietversendings of enige kombinasie van die voorafgaande.

SATRA hou homself besig met die fisieke regulering van die Suid-Afrikaanse Internet-ruggraat en sy Internet-verkeer deur 'n algemene eweknie-punt te skep. Enige diens in Suid-Afrika wat radio- of televisie-programme oor die Internet uitsaai, kan dit sonder 'n uitsaai-lisensie doen, maar moet dit deur 'n IDV met 'n VANS-lisensie van SATRA in terme van die Telekommunikasie Wet doen. Dus word die enigste regulering van die fisieke ruggraat van die Internet in Suid-Afrika deur die Telekommunikasie Wet uitgevoer (Buys, 2001: 414).

6.2 Internet-rolspelers en -organisasies in Suid-Afrika

Sedert die begin van die Internet in Suid-Afrika het die aantal rolspelers en organisasies in dié bedryf nie net beperk gebly tot die regering se regulerende rolspelers en organisasies nie. Daar is ook takke van internasionale Internet-organisasies wat in Suid-Afrika bedrywig is, asook belangrike nasionale Internet-rolspelers en –organisasies wat die Internet in Suid-Afrika vorm deur hul interne regulering.

Die Internet-rolspelers en -organisasies wat hier bespreek word is, Internet-diensverskaffers (IDV's), Telkom SA Bpk, ISPA (Internet Service Providers Association), SATRA (South African Telecommunications Regulatory Authority), USA (Universal Service Agency), SAIF (South African ISDN Forum), NNS (Nasionale Navorsingstigting) en Uninet, ISOC ZA (Internet Sociaty South Africa Chapter) en Domeinnaam-operateurs in Suid-Afrika. Die rol wat die Departement Kommunikasie speel in terme van regulering van die Internet word saam met die Elektroniese Kommunikasie en Transaksies Wet van 2002 by punt 6.3 bespreek (Buys, 2001: 29-33).

6.2.1 Internet-diensverskaffers (IDV's)

In die Suid-Afrikaanse konteks blyk dit dat daar 'n bestaande verskil tussen die definisies van "Internet-toegangsverskaffer" en "Internet-diensverskaffer" is, soos deur SATRA gedefinieer. "Internet-toegangsverskaffers" beteken die voorsiening van 'n Internet Protokol (IP) diens wat die ontvanger van die diens toelaat om toegang tot die wêreldwye Internet te verkry. Die breër term "Internet-diensverskaffers" verwys na beide toegang en diens soos e-pos, video-konferensies en inligtingsdiens.

Stellenbosch University http://scholar.sun.ac.za

Vir meer inligting oor IDV's in Suid-Afrika sien punt 6.2.3 waar ISPA (Internet Service Providers Association) bespreek word.

6.2.2 Telkom SA Bpk

Telkom SA Bpk het histories die eksklusiewe reg geniet om basiese telekommunikasie infrastrukture in terme van die Poskantoor Wet in Suid-Afrika tot stand te bring. Met die aanvang van die Telekommunikasie Wet het dit nie verander nie.

Telkom het in 1997 die lisensie gekry wat hom die reg gee om VANS (Value-Added Network Services) te voorsien, wat per definisie elektroniese data-wisseling, e-pos, protokol-omskakeling, toegang tot 'n databasis of bestuurde data-netwerkdiens, stempos, stoor en aanstuur faks, video-konferensies, telekommunikasie wat verband hou met uitgewery- en advertensie-dienste en elektroniese inligtingsdiense insluit.

Die PSTS-lisensie (Public Switched Telecommunications Service) van Telkom gee hom die eksklusiewe reg om sekere elemente van die PSTS te voorsien. Dit sluit in die Internasionale Telekommunikasie-diens en alle telekommunikasie-fasiliteite wat deur eneige persoon vir die voorsiening van VANS soos Internet-toegang gebruik word. Dus word toegangsverskaffers geforseer om die telekommunikasie-fasiliteite wat deur Telkom voorsien word, te gebruik.

Sedert 1996 verskaf Telkom deur SAIX (South African Internet Exchange) Internet-toegang. Aangesien SAIX slegs 'n toegangsverskaffer is en nie 'n diensverskaffer soos die meeste ander IDV's nie, is hul kostes baie laag. SAIX het ook die grootste aantal POP's (Point of Presence) oor die grootste geografiese gebied versprei in Suid-Afrika (Buys, 2001: 29-30).

6.2.3 ISPA (Internet Service Providers Association)

In Junie 1996 is ISPA gestig in reaksie op die waarneembare bedreiging van die onafhanklikheid van Internet-toegang wat deur Telkom se toetrede tot die Internet-toegangsmark meegebring is (Buys, 2001: 30-31).

ISPA is 'n nie-winsgewinde Suid-Afrikaanse Internet-bedryf-organisasie. Tans verteenwoordig ISPA ongeveer 50 IDV's (Sien Bylae C) met 'n wye verskeidenheid van dienste en teikenmarkte. Lede sluit nie-winsgewende verskaffers en opvoedkundige netwerke sowel as kommersiële diensverskaffers in ("About ISPA", 2002:2).

ISPA beheer die Suid-Afrikaanse ewekniepunte in Johannesburg (JINX) en Kaapstad (CINX) (Buys, 2001: 30-31). Dié ewekniepunte roeteer Internet-verkeer tussen die verskillende Internet-toegangsverskaffers en dien as 'n middel om die Suid-Afrikaanse Internet-verkeer binne die

Stellenbosch University http://scholar.sun.ac.za

landsgrense te hou. Dit verminder die onkoste van internasionale Internet-skakels en voorsien gebruikers van beter toegang tot Suid-Afrikaanse netwerke ("About ISPA", 2002:3).

Dit stel ISPA-lede in staat om hul interne Suid-Afrikaanse verkeer effektief te dra sonder om op ooreenkomste met die VSA en Europa staat te maak. In 1996 en 1997 het ISPA met 'n meerderheid stemme besluit om Telkom te verbied om met die ewekniepunte te skakel weens die politiese verdeeldheid tussen die organisasies. Dit het in 1998 verander toe alle toegangsverskaffers toegelaat is om van die ewekniepunte gebruik te maak (Buys, 2001: 30-31).

'n Besturende komitee wat uit verteenwoordigers van ISPA-lid-organisasies bestaan, is vir die bestuur van ISPA verantwoordelik. Dié komitee word deur die lede by ISPA se algemene jaarvergadering gekies.

Sedert sy ontstaan het ISPA 'n belangrike rol gespeel in die ontwikkeling van Suid-Afrikaanse telekommunikasie- en Internet-beleid. ISPA het aan beleidsgesprekke deelgeneem en verskeie voorleggings aan beleidsmakers van 'n aantal belangrike wetgewende prosesse gemaak, onder meer:

1. VANS en PTNS lisensiëring-regimes
2. Telkom waarde-oorsig
3. Telekommunikasie Wysigingswet
4. Elektroniese Kommunikasie en Transaksies Wet
5. Onderskepping en Monitering Wetsontwerp

ISPA is tans besig om sy Etiese Kode te finaliseer en sal aansoek doen om as 'n verteenwoordigende bedryfsliggaam in terme van die Elektroniese Kommunikasie en Transaksies Wet van 2002 herken te word ("About ISPA", 2002:3).

Volgens Die Grondwet van ISPA (sien Bylae D) is dit sy missie om 'n nie-winsgewende forum te verskaf waarbinne die belange van die Internet-diensverskaffers in Suid-Afrika gemeenskaplike kwessies kan bespreek sodat die gebruiker wêreldklas-diens kan ontvang en investeerders 'n billike wins op hul belegging kan kry ("Constitution of the Internet Service Providers' Association", 2002:3).

6.2.4 *SATRA (South African Telecommunications Regulatory Authority)*

SATRA is 'n statutêre liggaam wat deur seksie 5 van die Telekommunikasie Wet gestig is en is 'n regulerende waghond vir die telekommunikasie-bedryf. Een van die motiverende faktore vir die stigting van SATRA was om 'n telekommunikasie-omgewing te skerp waar daar 'n duidelike

Stellenbosch University http://scholar.sun.ac.za

skeiding tussen die funksie en kragte van die regering, telekommunikasie-operateurs en 'n reguleerder (SATRA) was om deursigtigheid en verantwoordelikheid aan te moedig.

SATRA is verantwoordelik vir die administrasie van regeringsbeleide, uitreiking van lisensies, bestuur van die radio-frekwensie-spektrum en die implementering van 'n wye verskeidenheid take wat deur die Telekommunikasie Wet onder die mandaat gebring is.

In 1997 het SATRA 'n grensverskuiwende uitspraak gelewer deurdat Internet-toegangsverskaffingsdienste in die werkkring van VANS en nie die PSTS, waarvoor Telkom eksklusiewe regte het, val nie. Telkom het dus geen aanspraak op eksklusiwiteit as dit by Internet-toegang kom nie (Buys, 2001: 31).

6.2.5 USA (Universal Service Agency)

USA is 'n statutêre liggaam wat in terme van seksie 58 van die Telekommunikasie Wet 103 van 1996 gestig is. Die missie van USA is om bekostigbare universele dienste en toegang tot Inligting en Kommunikasie Tegnologie dienste vir die minderbevoorregte gemeenskappe in Suid-Afrika te bevorder en te fasiliteer vir hulle ontwikkelling, bemagtiging en ekonomiese groei ("USA Background", 2002). Die visie van USA is om dié toegang te bevorder deur openbare bewustheid, navorsing en aanbevelings aan die Minister van Kommunikasie (Buys, 2001: 32).

Die organisasie funksioneer onder die regulering en beleidsraamwerk soos wat in die Wet se Wysiging van 2001 uiteengesit is. USA dien ook as die organisasie wat verantwoordelik is vir die implementering van Inligting en Kommunikasie Tegnologie-projekte van die Departement van Kommunikasie.

6.2.6 SAIF (South African ISDN Forum)

SAIF is in Julie 1995 gestig om die gebruik van ISDN tegnologie in Suid-Afrika te bevorder. ISDN werk soos 'n modem, maar is baie vinniger en gebruik spesiale telefoonlyne wat heelwat meer as gewone telefoonlyne kos. Sy doelwitte is om die gebruik van ISDN-oplossings te stimuleer, internasionale tendense en tegnologieë te monitor en die bekendstelling van ISDN in die kommersiële mark te bevorder. Lidmaatskap is oop vir alle partye wat betrokke is by die gebruik en verskaffing van ISDN kommunikasie en gereedskap (Buys, 2001: 32).

6.2.7 NNS (Nasionale Navorsingstigting) en Uninet

Die NNS is 'n statutêre liggaam wat in terme van die Nasionale Navorsingstigting Wet gevorm is en verenig die aktiwiteite van die voormalige Foundation of Research and Development en die Human Sciences Research Council.

Stellenbosch University http://scholar.sun.ac.za

Die NNS bestuur die Uninet-netwerk tussen akademiese instellings en navorsingsrade. Die Uninet-projek is in 1987 begin as 'n netwerk tussen die universiteite van Suid-Afrika en het 'n belangrike rol gespeel in die ontstaan van die Internet in Suid-Afrika. Uninet is met die VSA geskakel deur middel van 'n 3 Mb/s skakel en aan al die IDV's in Suid-Afrika (Buys, 2001: 33).

Sedert Februarie 2001 bestaan Uninet nie meer nie. Uninet se netwerk-verantwoordelikhede is aan TENET (Tertiary Education Network) oorgegee. TENET is 'n seksie 21-organisasie met die primêre doel om tot die voordeel van Suid-Afrikaanse universiteite en technikons Internet en inligtingstegnologiedienste te verseker deur:

1. kontrakte met diensverskaffers te bestuur
2. ondergeskikte operasionele funksies ter ondersteuning aan diensverskaffers te verskaf
3. ander toegevoegde waarde-dienste soos dit van tyd tot tyd nodig is ter ondersteuning van die hoër onderwyssektor in Suid-Afrika te voorsien ("Some facts about TENET", 2002:1).

6.2.8 *ISOC ZA (Internet Society Suid-Afrika Vergadering)*

Die Suid-Afrikaanse vergadering van die internasionale ISOC is in Oktober 1998 gestig en word amptelik deur ISOC erken. Vroeg in 1999 het ISOC ZA die lede van 'n naamspasie-ontwerpkomitee gekies om 'n beleidsontwerp vir die top-vlak .za domeinnaam saam te stel (Buys, 2001: 33).

Volgens ISOC ZA se grondwet (Sien Bylae E) is die doel van die organisasie:

1. om die belange van die Suid-Afrikaanse deel van die wêreldwye Internet-gemeenskap te dien
2. om samewerking en dialoog tussen ISOC ZA as 'n verteenwoordiger van die Suid-Afrikaanse Internet-gemeenskap, Internet-diensverskaffers, reguleringsorganisasies en ander belangstellende partye te bewerkstellig
3. om deelname aan en/of borgskappe van kongresse, seminare en werkswinkels te reguleer ("The Constitution of the South African Chapter", 2002: 22-23).

Namespace ZA is 'n organisasie wat gestig is as gevolg van samewerking tussen die voormalige administrateur van die .za domein, Mike Lawrie, en ISOC ZA vir beter verteenwoordiging van die Suid-Afrikaanse Internet-gemeenskap. In Augustus 2001 het Namespace ZA sy stigtingsvergadering gehou. Dit was die gevolg van die naamspasie-ontwerpkomitee wat in 1999 die beleidsontwerp moes saamstel vir die top-vlak .za domeinnaam ("Namespace ZA", 2002:3).

Stellenbosch University http://scholar.sun.ac.za

6.2.9 *Domeinnaam operateurs in Suid-Afrika*

Suid-Afrika is deur IANA (Internet Assigned Numbers Authority) die .za-domeinnaam-spasie toegeken. Uninet administreer die top-vlak .za-domein. 'n Reeks organisasies en individue bestuur die volgende tweede-vlak domeine in Suid-Afrika (Buys, 2001: 33-34):

1. .AC.ZA — vir Suid-Afrikaanse navorsing- en akademiese instellings. Administrasie van die domein word deur TENET hanteer. Netwerke wat binne die .ac.za naamspasie val, word nie verplig om lede van TENET te wees nie. Die administrateur van AC.ZA domein is Duncan Martin: e-pos: dhm@tenet.ac.za. Webwerf: http://www.tenet.ac.za/ac_za/index.htm.
2. ALT.ZA — nog geen definisie beskikbaar nie. Die administrateur van ALT.ZA is Alan Barrett: e-pos: hostmaster@alt.za.
3. .BOURSE.ZA — vir alle Suid-Afrikaanse ondernemings wat op die Johannesburgse Effektebeurse geregistreer is. Registrasie is onderhewig aan bewyse van wettige eienaarskap van die onderneming se naam en bewyse dat die onderneming op die Johannesburgse Effektebeurs gelys is. Vir meer inligting: http://www.i.bourse.za.
4. .CITY.ZA — vir plaaslike en ander verwante organisasies (munisipaliteite, distriksrade, ens) binne Suid-Afrika wie se doel dit is om plaaslike gemeenskappe se belange te dien. Die administrateur is Pieter Geldenhuys: e-pos: geldepa@unisa.ac.za.
5. .CO.ZA — vir kommersiële organisasies. Die domein stem baie ooreen met die .COM domein van die Internet en word deur UniForm Association bestuur. Webwerf: http://co.za/.
6. .EDU.ZA — vir afstandsonderrig-organisasies. Die domein administrateur is Theuns Laubscher: e-pos: theuns@icg.edu.za. Webwerf: http://edu.za.
7. .GOV.ZA — vir regeringsdepartemente. Die registrasievorm kan by die webwerf gekry word: http://dnsadmin.gov.za/
8. .LAW.ZA — vir organisasies en individue wat in die regsbedryf betrokke is. Registrasie kan deur die Kaapse Regsvereniging gedoen word. Webwerf: http://www.law.za.
9. .MIL.ZA — vir militêre instellings. Webwerf vir meer inligting: http://www.mil.za.
10. .NET.ZA — vir die gebruik van die netwerk infrastruktuur van IDV's in Suid-Afrika. Dit kan ook deur 'n IDV-gasheer gebruik word. Onderhandeling word gevoer vir 'n nuwe administrateur van die domein. Tot verdere kennisgewing is nuwe registrasies vir die domein opgeskort.
11. .NGO.ZA — slegs vir nie-regeringsorganisasies. E-pos die domein se administrateur by: dnsadmin@sn.apc.org.

Stellenbosch University http://scholar.sun.ac.za

12. .NOM.ZA — vir individue, persoonlike name en nie vir organisasies nie. Die administrateur is Mike Jensen: e-pos: mikej@sn.apc.org.
13. .ORG.ZA — vir nie-kommersiële organisasies. Webwerf: http://www.org.za/.
14. .SCHOOL.ZA — vir skole. Webwerf: http://www.school.za/.
15. .TM.ZA — vir die wetlike eienaars van geregistreerde handelsmerke. Webwerf: http://www.tm.za/.
16. .WEB.ZA — vir individue en organisasies wat slegs 'n naamspasie nodig het vir Internet-diensrekenaars. Kontak die administrateur vir registrasie by hostmaster@web.za.

Netwerke wat ZA domeinname het, moet in Suid-Afrika gebaseer wees. Mense wat vir 'n domein wil aansoek doen, moet kennis dra van die standaarde vir Internet-domeine (".ZA domain space", 2002:1-6).

6.3 Elektroniese Kommunikasie en Transaksies Wet van 2002

Die Elektroniese Kommunikasie en Transaksies Wetsontwerp wat aan die begin van 2002 vir kommentaar van belanghebbendes verskyn het, het 'n wankelrige pad gehad totdat dit wet geword het. Alhoewel daar baie dele van die Wet is wat kritiek ontvang het, het geen deel van die Wet so baie kritiek soos Hoofstuk 10 ontvang nie. In dié hoofstuk word die stigting van 'n agentskap vir domeinname voorgestel wat beheer oor die plaaslike .za domein, Suid-Afrika se top-vlak domein, sal oorneem van Mike Lawrie en Namespace ZA wat tot en met die inwerkingstelling van die nuwe Wet in beheer was van dié domein (De Wet, 2002).

6.3.1 Wat behels die Wet?

Die algehele doel van die Elektroniese Kommunikasie en Transaksies Wet van 2002 (sien Bylae F) is om elektroniese transaksies moontlik te maak en te fasiliteer deur regsekerheid rondom die transaksies en kommunikasie wat elektronies gedoen word, te verseker. Die belangrike sake wat deur die Wet gedek word, sluit in:

1. Die maksimisering van voordele deur deelname van klein-, medium- en mikro-ondernemings (SMME's). Dit sal SMME's in staat stel om globale verhoudings met handelsvennote enige plek ter wêreld te smee.
2. Verskeie meganismes moet in werking gestel word deur mense uit voorheen benadeelde gemeenskappe te betrek om doeltreffende deelname in e-handel te bevorder. Dit sluit die nasionale e-strategie in.
3. Regsekerheid deur te verseker dat elektroniese kommunikasie erken word deur die Wet. Met die regsekerheid wat die Wet skep, word daar ongekende groei in elektroniese transaksies verwag.

Stellenbosch University http://scholar.sun.ac.za

4. Die totstandkoming van 'n akkrediteringsliggaam om met die ontwerp en die ontwikkeling van prosedures, stelsels en standaarde te help vir akkreditering. Dit sal akkrediteringskriteria, verwagte diensvlakke, monitering, staking van akkreditasie, terugvoeringstelsels en administrasie insluit.
5. Die stigting van 'n kriptografiese register wat 'n rekenaarstelsel is wat gebruikers in staat stel om hul kriptografiese tegnologie te registreer. Kriptografie is die proses van digitale "skommeling" van data wat dan uit geheime sleutels bestaan.
6. Wettoepassing om rekenaarmisdade te voorkom deur die aanstelling van kuberinspekteurs.
7. Effektiewe bestuur van Internet-verwante sake deur die stigting van 'n behoorlike bestuursregime met betrekking tot domeinname in Suid-Afrika en die beperking van die verantwoordelikheid van Internet-diensverskaffers ("ECT Bill", 2001: 39).

Die wet behels die volgende:

- **Hoofstuk 1: Interpretasie, doelwitte en toepassings** - Dié hoofstuk definieer kritieke woorde, frases en terme en stel die hoofdoelwitte van die Wet uiteen ("ECT Bill", 2001: 39).
- **Hoofstuk 2: Maksimiseringsvoordele en beleidsraamwerk** - Die doelwit is om die voordele wat die Internet bied, te maksimiseer deur universele en bekostigbare toegang vir almal te bied ("ECT Bill", 2001: 39).
- **Hoofstuk 3: Fasilitering van elektroniese transaksies** - Die hoofstuk handel oor die verwydering van regsversperrings tot elektroniese transaksies ("ECT Bill", 2001: 39).
- **Hoofstuk 4: E-regeringsdienste** - Die hoofstuk fasiliteer elektroniese liassering. Dit lys die vereistes vir die produksie van elektroniese dokumente en die integriteit van inligting. Voorsiening word gemaak vir 'n Departement of Ministerie om dokumente in die vorm van elektroniese data-boodskappe te aanvaar en te stuur, permitte en lisensies in die vorm van databoodskappe uit te reik en betaling in elektroniese vorm te ontvang ("ECT Bill", 2001: 40).
- **Hoofstuk 5: Kriptografie-verskaffers** - Die Internet voorsien sekere sekuriteits-uitdagings wat sonder die nodige reguleringsraamwerk 'n gevaar vir die sekuriteit van gebruikers en die land kan inhou. Die Hoofstuk eis van die verskaffers van kriptografie-materiaal om op die voorgeskrewe manier hul naam en adresse, die name van hul produkte en 'n kort beskrywing daarvan aan die Departement Kommunikasie te voorsien. Dit sal die ondersoek-agentskappe help om enkripsie-boodskappe te ontsyfer ("ECT Bill", 2001: 40).
- **Hoofstuk 6: Bekragtigingsdiensverskaffers** - Identifisering en bekragtiging van die partye in die kuberruim bly 'n uitdaging en hou 'n gevaar in vir gebruikers en ondernemings ("ECT Bill", 2001: 40).

Stellenbosch University http://scholar.sun.ac.za

- **Hoofstuk 7: Gebruikersbeskerming** - Verkopers moet gebruikers van 'n minimum stel inligting verskaf wat insluit die prys van die produk of diens, kontakbesonderhede en die reg om van die elektroniese transaksie te onttrek voordat dit voltooi is. Gebruikers is ook onder sekere omtstandighede geregtig op 'n "afkoel"-periode waarin hulle sekere soorte transaksies wat elektronies voltooi is, kan kanselleer sonder enige boeteS ("ECT Bill", 2001: 40).

- **Hoofstuk 8: Persoonlike inligting en privaatheidsbeskerming** - Die hoofstuk bring 'n vrywillige regime van beskerming van persoonlike inligting tot stand. Ontvangers van persoonlike inligting (data-insamelaars) mag hulle aan unverseel-aanvaarde data-beskermingsbeginsels onderskryf. Daar word gereken dat gebruikers eerder slegs met dié data-insamelaars sal werk wat volgens die beginsels werk ("ECT Bill", 2001: 40).

- **Hoofstuk 9: Beskerming van kritieke databasisse** - Kritieke datainligting kan 'n risiko vir die nasionale sekuriteit van die land inhou of die ekonomiese en sosiale welstand van die land se inwoners, as dit blootgestel word. Die Minister mag sekere sake wat verband hou met die registrasie van kritieke databasisse voorskryf en sekere prosedures en tegnologiese metodes wat in hul berging en argivering gebruik word, eis ("ECT Bill", 2001: 40).

- **Hoofstuk 10: Domeinnaam-agentskap en administrasie** - 'n Seksie 21-onderneming sal gestig word om die domeinnaam-spasie van Suid-Afrika te bestuur. Sy lidmaatskap en reguleringstrukture moet verteenwoordigend van die algemene Suid-Afrikaanse gemeenskap, die regering en deelnemers wees. Daar word in die Wet voorsiening gemaak vir die doelwitte, magte en funksies van die agentskap. Daar is ook voorsiening gemaak vir alternatiewe resolusie-metodes vir dispute wat oor domeinname gaan. Die Minister is gemagtig om 'n nasionale beleid vir die .za domeinnaam spasie te formuleer ("ECT Bill", 2001: 41).

- **Hoofstuk 11: Beperkings van die verantwoordelikheid van diensverskaffers** - Die hoofstuk handel oor die beperkings van die verantwoordelikheid van diensverskaffers en skep 'n veilige vesting vir diensverskaffers wat tans tot 'n wye verskeidenheid potensiële aanspreeklikhede blootgestel is, bloot deur hul basiese tegniese funksies na te kom. Die diensverskaffers mag hul verantwoordelikheid beperk waar hulle bloot as "pype" vir die versending van data-boodskappe was. In elke situasie voorsien die Wet spesifieke vereistes waaraan die handelings van die diensverskaffers moet voldoen voordat hulle hul verantwoordelikheid kan beperk ("ECT Bill", 2001: 41).

- **Hoofstuk 12: Kuberinspekteurs** - Die Departement kan volgens die hoofstuk van die Wet kuberinspekteurs aanstel. Dié kuberinspekteurs kan op Internet-webwerwe rondloer en onder meer krakers en mense wat bedrog pleeg, monitor. Die inspekteurs gaan by magte wees om fisieke- en kuber-gebiede te deursoek en kan op eiendom beslag lê, afhangend of daar 'n bevel uitgereik is.

Stellenbosch University http://scholar.sun.ac.za

Hulle kan ook gevra word om die polisie of ander ondersoekliggame by te staan ("ECT Bill", 2001: 41).

- **Hoofstuk 13: Kubermisdaad** - Die Wet skep die eerste statutêre voorsorgmaatreëls ten opsigte van kubermisdaad in Suid-Afrikaanse jurisprudensie. Nuwe statutêre misdade wat betrekking het op inligtingstelsels word bekendgestel, onder meer:

    1. ongemagtigde toegang tot data
    2. onderskepping of inmenging met data
    3. rekenaarverwante afpersing
    4. bedrog
    5. vervalsing

Enige persoon wat 'n ander persoon aanhits of help om enige van die misdade te pleeg, sal skuldig bevind word as 'n medepligtige tot die misdaad ("ECT Bill", 2001: 41).

6.3.2 Kommentaar op dele van die Wet

Die groot regtelike onsekerheid wat in Suid-Afrika geheers het, is met die verordening van die Elektroniese Kommunikasie en Transaksies Wet 25 van 2002 verwyder. Die primêre doel van die Wet soos reeds by 6.3.1 genoem, is om elektroniese transaksies moontlik te maak en te fasiliteer deur regsekerheid rondom die transaksies en kommunikasies wat elektronies gedoen word, te verseker. Hiervoor maak die Wet vir elke moontlike aspek wat betrekking het op die elektroniese omgewing voorsiening (Jansen, 2002:2).

Volgens 'n petisie wat mnr. Ryk Meiring (2002) namens die Information Technology Lawyers' Forum op 10 Julie 2002 aan President Thabo Mbeki gerig het, is die Wetsontwerp ten spyte van groot publieke kommentaar sonder die nodige wysigings aanvaar (Meiring, 2002:1). "Terwyl daar sommige hoofstukke is wat goed ontwerp is, is daar baie met tekortkominge in terme van tegniese, wetlike en logiese aspekte" skryf Meiring in sy petisie (Meiring, 2002:1).

Alhoewel die Departement Kommunikasie verskeie aanbevelings en kommentaar op die wetsontwerp van belanghebbendes soos Namespace ZA ontvang het, word daar in dié studie slegs Meiring (2002) se petisie gefokus.

Meiring (2002) glo sommige dele van die Wetsontwerp se tekortkominge is van so 'n aard dat dit die aktiwiteite waarvoor die Wet ontwerp is, sal onderdruk. Ander is glo nagemaak en onnodig en plaas geweldige onkostes op die Suid-Afrikaanse ekonomie wat nie tot die regering of sy burgers se voordeel strek nie. Volgens Meiring is daar ander dele van die Wetsontwerp wat ingrypende en ongedefinieerde nuwe magte aan die Minister van Kommunikasie toeken. Dié nuwe

Stellenbosch University http://scholar.sun.ac.za

magte word nie aan voldoende toesig en wigte en teenwigte onderwerp nie en is dus vatbaar vir misbruik (Meiring, 2002:1).

- **Hoofstuk 1 en 2** van die Wetsontwerp het nie veel kommentaar uitgelok nie en is in die algemeen deur diegene wat kommentaar gelewer het, ondersteun. Alhoewel Namespace ZA breedvoerig kommentaar gelewer het op Hoofstuk 1 se definisies is die meeste van die voorstelle aangepas en is nou deel van die Wet ("Comments on the ECT Bill by Namespace ZA", 2002:2).

- **Hoofstuk 4: E-regeringsdienste** - Meiring (2002) glo die hoofstuk is progressief en aanloklik en bring Suid-Afrika in pas met die mees gesofistikeerde regerings ter die wêreld (Meiring, 2002:5).

- **Hoofstuk 8: Beskerming van persoonlike inligting** - Volgens Meiring (2002) is die hoofstuk van geen waarde nie, aangesien die nakoming van die hoofstuk vrywillig is. Alhoewel Meiring geen probleem het met hoe die hoofstuk uiteengesit is nie, voel hy tog die hoofstuk kan uit die Wet uitgelaat word (Meiring, 2002: 9).

- **Hoofstuk 9: Beskerming van kritieke databasisse** – Dié hoofstuk gee die Minister van Kommunikasie wye en aanvallende magte om na goeddunke te handel wat volgens Meiring (2002) deur die Grondwet van Suid-Afrika uitgedaag kan word. Die identifisering van kritieke data en kritieke databasisse punt (53) is maar net een voorbeeld van die omvattende magte wat aan die Minister in die hoofstuk toegeken word (Meiring, 2002: 10):

> **53.** The Minister may by notice in the *Gazette* -
>
> (a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data for the purposes of this Chapter; and
> (b) establish procedures to be followed in the identification of critical databases for the purpose of this Chapter ("Electronic Communications and Transactions Act", 2002)

- **Hoofstuk 10: Domeinnaam-agentskape en -administrasie** – Die hoofstuk ken ongekende magte aan die Minister van Kommunikasie toe wat die beheer en administrasie van die .za domeinnaam betref. Sommige belanghebbende glo dat as die regering die bestuur van die land se ccTLD ("country code Top-Level Domain") wil oorneem en daar ontstaan enige haakplekke, sal mense eenvoudig begin om hul domeinname elders te registreer. Namespace ZA se kommentaar op Hoostuk 10 beskou seksie 61 (2) as onaanvaarbaar, omdat dit nie volgens die normale model van seksie 21-ondernemings hanteer word nie ("Comments on the ECT Bill by Namespace ZA", 2002: 5).

Stellenbosch University http://scholar.sun.ac.za

> **61.** (2) Notwithstanding the Companies Act, 1973, an amendment to the memorandum of association or articles of association affecting any arrangement made by any provision of this Chapter, does not have any legal force and effect unless the Minister has consented in writing to such an amendment, which consent may not be withheld unreasonably ("Electronic Communications and Transactions Act", 2002).

Namespace ZA voel ook die samestelling van die domeinnaam-agentskap moet mense met DNS-kennis insluit, om te verseker dat die .za-domein aan die internasionaal aanvaarde tegeniese standaarde voldoen. Hiervoor maak die Wet nie voorsiening nie ("Comments on the ECT Bill by Namespace ZA", 2002):

> **62.** (3) (b) Sectors of stakeholders contemplated in subsection (2)(d) are -
>
> (i) The existing Domain Name community;
> (ii) Academic and legal sectors;
> (iii) Science, technology and engineering sectors;
> (iv) Labour;
> (v) Business and the private sector;
> (vi) Culture and language;
> (vii) Public sector;
> (viii) Internet user community ("Electronic Communications and Transactions Act", 2002).

Deel 3 van dié hoofstuk gee die Minister van Kommunikasie weer eens wye en omvattende magte om na goeddunke met die .za naamspasie te handel. Namespace ZA (2002) glo dis 'n ongesonde benadering.

> **65.** (1) The Authority must -
>
> (a) publish guidelines on -
> (i) the general administration and management of the .za domain name space;
> (ii) the requirements and procedures for domain name registration; and
> (iii) the maintenance of and public access to a repository, with due regard to the policy directives which the Minister may make from time to time by notice in the *Gazette* ("Electronic Communications and Transactions Act", 2002).

Meiring (2002) glo die regering se beheer oor die .za domein sal 'n degradasie in die huidige aanlyn-status van dié domein tot gevolg hê. Hy is ook bekommerd oor die gebrek aan deursigtigheid en verantwoordelikheid wat die lede van die voorgestelde agentskap sal hê (Meiring, 2002).

- **Hoofstuk 11: Beperkings van die verantwoordelikheid van diensverskaffers -** Volgens Meiring (2002) is dié 'n verligte benadering tot die kwellende vraag of Internet-diensverskaffers en

Stellenbosch University http://scholar.sun.ac.za

ander bemiddelaars wetlik verantwoordelik gehou kan word vir die inligting wat hulle onwetend stoor en versend. Die hoofstuk verskaf voldoende beskerming aan alle partye wat deur die potensiële verantwoordelikheid geraak word, wat uit die onwettige inhoud of kommunikasies na vore kan kom (Meiring, 2002:14).

- **Hoofstuk 12: Kuberinspekteurs** – Dié hoofstuk se bedoeling is prysenswaardig, volgens Meiring (2002) maar die rol van polisiëring moet aan die Suid-Afrikaanse Polisiediens oorgelaat word en dan in besonder die huidige Rekenaar-misdaad-eenheid. Om 'n parallelle diens soos die kuberinspekteurs in te stel, wat nie 'n voldoende stelsel van wigte en teenwigte het nie, voorsien die Departement Kommunikasie van 'n ongeoorloofde uitbreiding van sy magte.

- **Hoofstuk 13: Kubermisdaad** - Meiring (2002) beskou die hoofstuk as noodsaaklik en goed uiteengesit. Hy glo egter dat die definisie van kubermisdaad dalk breër is as na die wense van die Internet-gemeenskap. Meiring sê in die gevolgtrekking van sy petisie:

> "Ons is van mening dat baie van die bepalings van die Wet 'n ongemagtigde en ongewenste poging is om die afhanklikheid van die Ministerskap van Kommunikasie en sy Departement te verleng, verteenwoordig en om sy beheer oor privaatsektor-aktiwiteite tot 'n onredelike omvang te vermeerder en om vir homself uitgebreide magte om na goeddunke te handel sonder behoorlike oorsig, te skep" (Meiring, 2002: 16).

Dit is heeltemal begryplik dat Suid-Afrika die Afrika-kontinent in die uitreiking van elektroniese handel- en Internet verwante wetgewing sal lei. Daarom is dit belangrik dat die model wat Suid-Afrika voorstel en implementeer sonder enige foute/leemtes is (Meiring, 2002).

6.4 Kopiereg in Suid-Afrika

Die aktiwiteite wat in terme van die Kopiereg Wet van 1978 beskerm word, word spesifiek in die Wet gelys en gedefinieer. Dit sluit die volgende in:

1. literêre, musikale en kunswerke
2. klankopnames, rolprente, klank- en televisie-uitsending en programdraende seine
3. publikasies
4. rekenaarprogramme

Rekenaardatabasisse word beskerm as literêre werke. Internet-webwerwe is gewoonlik multimedia-produkte wat as literêre werke, kunswerke, musikale werke en rekenaarprogramme beskerm word.

Stellenbosch University http://scholar.sun.ac.za

'n Werk moet oorspronklik wees om volgens die Suid-Afrikaanse Kopiereg Wet van 1978 kopiereg te hê. Dit beteken die werk mag nie van ander bronne gekopiëer word nie, maar moet 'n produk van die outeur se eie pogings wees.

Die werking van die Kopiereg Wet is verleng deur 'n proklamasie in terme van seksie 37 na alle lande wat lede van die Bern Konvensie is wat in 'n bylae tot die proklamasie gelys is. Die Bern Konvensie is 'n internasionale konvensie oor die regulering van intellektuele eiendomsreg. Verwysings na die Suid-Afrikaanse Kopiereg Wet moet daarom in die lig daarvan geïnterpreteer word. Alhoewel die Bern Konvensie slegs van toepassing is op literêre en kunswerke is die proklamasie van toepassing op alle soorte werke wat in die Kopiereg Wet gedefinieer word (De Villiers, 2001: 42).

Volgens die Kopiereg Wet van 1978 sal die outeur die reg hê om outeurskap te eis van die werk en om beswaar te maak teen enige vervorming, skending en ander veranderings daaraan, waar sulke handelinge afbreuk doen aan die eer en reputasie van die outeur. Nieteenstaande die oordrag van die kopiereg in 'n literêre, musikale of kunswerk, 'n rolprent of rekenaarprogram nie. Die belangrikste elemente van die morele regte wat in die Kopiereg Wet verskyn, is die outeurskapreg, wat die reg is om as die outeur van die werk geïdentifiseer te word en die integriteitreg, om beswaar te maak teen die nadelige behandeling van die werk (De Villiers, 2001: 45-46).

6.4.1 *Kopieregoortreding op die Internet*

Oortreding van kopiereg word in seksie 23 van die Kopiereg Wet hanteer. Dit maak voorsiening vir die oortreding van kopiereg wanneer 'n persoon wat nie die eienaar van die kopiereg is nie enige handelinge doen waarvoor die eienaar 'n eksklusiewe reg het om te doen of ander toestemming kan gee om dit te doen, of veroorsaak dat ander dié handelinge doen. Daar is 'n verskeidenheid aktiwiteite op die Internet wat die moontlikheid het om kopiereghouers se regte te skend.

- **Oortreding deur reproduksie** - Die kopiereghouers het in terme van die Kopiereg Wet die eksklusiewe reg om te reproduseer of om reproduksie van enige wyse of vorm van bykans al die verskillende tipes werk wat deur die Wet beskerm word, goed te keur. Die eksklusiewe reproduksie-regte wat aan die kopiereghouers toegestaan word, is baie wyd, aangesien dit voorsiening maak vir reproduksie van enige wyse en vorm. Deur hul werk op 'n webwerf te plaas, moet kopiereghouers 'n nie-eksklusiewe lisensie aan alle Internet-gebruikers wat toegang tot die materiaal het, toeken sodat kortstondige kopieë van die materiaal op hul rekenaars gemaak kan word, soos reeds in Hoofstuk 5 by 5.4 bespreek is (De Villiers, 2001: 47).

- **Oortreding deur publikasie** - In terme van die Kopiereg Wet word literêre, musikale en kunswerke en rekenaarprogramme beskerm deurdat die kopiereghouer die eksklusiewe reg het om

Stellenbosch University http://scholar.sun.ac.za

eerste te publiseer of om die publikasie van die werk goed te keur. 'n Werk word as gepubliseer beskou wanneer daar kopieë van die werk gemaak is en aan die publiek beskikbaar gestel is. Dit beteken dat die uitreiking of beskikbaarstelling van kopieë van 'n literêre, musikale en kunswerk of 'n rekenaarprogram op 'n webwerf, as publikasie beskou word (De Villiers, 2001: 49-50).

- **Oortreding deur ongemagtigde handel** - Indirekte of sekondêre skending van 'n werk vind plaas wanneer 'n persoon, sonder die lisensie van die kopiereghouer, so 'n werk vir nie-private gebruik inspan, of verkoop, of die werk te koop aanbied of die werk versprei vir handelsdoeleindes of vir enige ander doel die werk versprei op so 'n manier dat dit nadelig vir die kopiereghouer is. Dit word as kopieregskending beskou. Dit is ook van toepassing op werke wat oor die Internet aangeskaf word (De Villiers, 2001: 51).

- **Oortreding deur 'n aanpassing van die werk te maak** - Om 'n aanpassing van 'n literêre, musikale en kunswerke of 'n rekenaarprogram te maak, val ook binne die eksklusiewe regte van die kopiereghouer. 'n Aanpassing in terme van literêre werke sluit in vertaling en om 'n skets/prent-weergawe te maak. In terme van musikale werke sluit dit enige toonsetting of transkripsie in. In terme van 'n kunswerk sluit dit enige transformasie van die werk in wat op so 'n wyse gedoen is dat die oorspronklike of 'n substansiële kenmerk van die oorspronklike herkenbaar bly. In terme van 'n rekenaarprogram sluit dit 'n weergawe van die program in ander programmeertaal-kode, of 'n notasie of fiksasie van die program in 'n ander medium as die oorspronklike. Die kode van 'n webwerf in HTML, JavaScript of ander kodes moet dus gesien word as 'n rekenaarprogram. Die ontwerp, uitleg en konstruksie van die webwerf kan daarom teen aanpassings beskerm word (De Villiers, 2001: 54).

Die Internet verskaf unieke geleenthede vir kopieregskending wat regoor die wêreld probleme veroorsaak. Dié verskillende probleem-areas van kopiereg op die Internet is reeds in Hoofstuk 5 bespreek by 5.4.1.

Daar is al baie gevra of Internet-diensverskaffers verantwoordelik gehou moet word indien intekenare materiaal op hul webwerf plaas wat kopiereg skend. In terme van die Kopiereg Wet is 'n persoon wat 'n ander persoon veroorsaak of toestemming gee om sy Internet-diens te gebruik om kopieë van kopieregte werk te versprei, ook verantwoordelik vir die oortreding.

Volgens die Kopiereg Wet is IDV's en gashere dan ook aanspreeklik as hulle so iets wetend en selfs onwetend toelaat (De Villiers, 2001: 47). Die Elektroniese Kommunikasies en Transaksies Wet van 2002 maak in Hoofstuk 11 egter voorsiening vir die beskerming van IDV's teen dié verantwoordelikheid vir ander se oortredings ("Comments on the ECT Bill by Namespace ZA", 2002). In dié hoofstuk van die Wet word voorsiening gemaak vir diensverskaffers se "pyp"-funksie tussen die sender en ontvanger van data (seksie 73), die stoor van data in sy kasgeheue (seksie 74),

Stellenbosch University http://scholar.sun.ac.za

sy funksies as gasheer-rekenaar (seksie 75) en soek-enjin (seksie 76). Volgense seksie 78 van die hoofstuk in die Wet is diensverskaffers onder geen algemene moniteringsverpligting nie:

> **78.** (1) When providing the services contemplated in this Chapter there is no general obligation on a service provider to -
>
> (a) monitor the data which it transmits or stores; or
> (b) actively seek facts or circumstances indicating an unlawful activity.
>
> (2) The Minister may, subject to section 14 of the Constitution, prescribe procedures for service providers to -
>
> (a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and
> (b) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service ("Electronic Communications and Transactions Act", 2002).

6.4.2 Gevallestudie: M-Web Afrikaans vs. watkykjy.co.za

Vir ongeveer twee weke aan die begin van 2001 het watkykjy.co.za begin met 'n blatante aanslag op M-Web Afrikaans se gespreksforum. Die aanval op M-Web Afrikaans het gegaan oor hul gebruik van "Ou Koeie" as verwysing na die argief. Volgens die webmeesters van watkykjy.co.za het hulle die "Ou Koeie" verwysing na die argief op hul webwerf eerste teen 2000 gebruik en dat M-Web Afrikaans wat dit sedert 1999 gebruik by hulle gesteel het. M-Web Afrikaans is eers per e-pos gekontak oor die saak. Ná twee dae nadat watkykjy.co.za nog geen antwoord van M-Web Afrikaans terug gekry het nie, het watkykjy.co.za met sy aanslag begin deur blatante advertering van watkykjy.co.za op M-Web Afrikaans se gespreksforum. Die vloei van gedagtes op die forum ontwrig deur sinlose boodskappe.

Die bestuurder van M-Web Afrikaans op daardie stadium, Pieter Redelinghuys, het ná 'n paar dae 'n e-pos aan watkykjy.co.za gestuur waarin hy skryf:

> "Ek versoek watkykjy.co.za se volgelinge vriendelik om maar die ou koeie storie saam met die strydbyle te begrawe, sodat M-Web Afrikaans se gebruikers aan die onderwerp van bespreking kan deelneem" ("Wkj? en M-Web Afrikaans", 2001).

Op dieselfde dag het die vorige bestuurder van M-Web Afrikaans, Stefanie Hefer, ook 'n e-pos aan watkykjy.co.za gestuur waar sy die oorsprong van die "Ou Koeie"-skakel op M-Web Afrikaans verduidelik.

Redelinghuys en Hefer se e-pos boodskappe is op watkykjy.co.za se webwerf geplaas saam met 'n storie "Wkj? en M-Web Afrikaans slaan vuis" en skakels na M-Web Afrikaans se

Stellenbosch University http://scholar.sun.ac.za

gespreksforum waar watkykjy.co.za blatant hulself adverteer het en sinvolle gesprekke op die forumbord onmoontlik gemaak het ("Wkj? en M-Web Afrikaans", 2001).

Dié gevallestudie is nie werklik 'n kopiereg-kwessie nie, maar bevat tog elemente van intellektuele eiendomsreg, handelsmerkskending en laster. Alhoewel daar geen formele klag van enige van die twee partye teen die ander gemaak is nie, is dit tog 'n betreklik aktuele gevallestudie om te bestudeer.

Die Kopiereg Wet is glad nie hier ter sprake nie, aangesien altwee webwerwe'n bekende idioom, "Moenie ou koeie uit die sloot grawe nie", gebruik het om tot by die Ou Koeie-skakel in hul argief te kom. Nie een van die webwerwe het dus wetlik aanspraak op die alleenreg van die "Ou Koeie"-skakel nie. Hefer het 'n volledige skriftelike antwoord aan watkykjy.co.za gestuur, waarin sy van haar kant af die hele geskil besleg het. Haar brief is volledig op watkykjy.co.za gepubliseer met 'n verskoning van watkykjy.co.za aan Hefer. Dit is duidelik uit die voorafgaande dat M-Web Afrikaans het van die self-reguleringsmetode gebruik gemaak om die situasie op te los (Hefer, persoonlike kommunikasie, Januarie 8, 2003).

6.5 Handelsmerke en domeinname

'n Domeinnaam is 'n bate vir enige onderneming aangesien dit dieselfde doel dien as 'n handelsmerk in die "aflyn"-wêreld (Silber, 2000). Handelsmerke en domeinname is reeds in hoofstuk 5 by 5.5 bespreek.

Die domeinnaam southafrica.com behoort aan 'n Amerikaanse maatskappy, Virtual Countries. Reinhardt Buys van Buys Inc. het in *Die Burger* (2003) gewaarsku dat dit "'n wonderwerk" sal kos om "Suid-Afrika uit die hande van die Amerikaners terug te kry". Dit volg ná die Nieu-Seelandse regering in Desember 2002 sy stryd verloor het om beheer oor die domeinnaam newzealand.com van Virtual Countries terug te kry.

Reeds in 1995 het Virtual Countries die meeste lands- en geografiese name geregistreer, lank voordat die onderskeie regerings die waarde van die Internet as bemarkingsgereedskap raakgesien het. Die Nieu-Seelandse regering het in 2002 met 'n arbitrasieprosedure by World Intellectual Property Organization (WIPO) begin om die domeinnaam terug te kry. Die Nieu-Seelanders het daarop aanspraak gemaak, omdat "New Zealand" 'n handelsmerk is wat aan die regering van die land behoort. WIPO het in sy uitspraak gesê aanduidings van geografiese oorsprong kan nie op sigself as handelsmerke beskou word nie.

Al oplossing nou vir regerings en ander instansies is om so gou moontlik domeinname vir die geografiese-name van die land soos stede, riviere, berge, ens. te registreer voordat dit buite die

Stellenbosch University http://scholar.sun.ac.za

regulering van die regering kom. Daar bestaan geen regulering wat mense buite die land of wat geen aanspraak op die name het nie, verbied om dit te registreer nie (Louw, 2003: 3).

6.5.1 Geregistreerde- en ongeregistreerde handelsmerke

Handelsmerke kan in geregistreerde en ongeregistreerde handelsmerke ingedeel word. 'n Geregistreerde handelsmerk kan 'n "device", naam, handtekening, woord, letter, nommer, vorm, konfigurasie, patroon, ornamentasie, kleur, houer vir goedere of enige kombinasie van dié wees. In terme van die Handelsmerk Wet 194 van 1993 sal skending van 'n handelsmerk plaasvind wanneer:

1. 'n identiese merk, of 'n merk wat amper die geregistreerde handelsmerk verteenwoordig wat moontlik kan mislei of verwarring veroorsaak, gebruik word om handel mee te dryf met die goedere en dienste waarvoor die handelsmerk geregistreer is, sonder die toestemming van die handelsmerk-eienaar.
2. 'n identiese of soortgelyke merk gebruik word terwyl handel gedryf word met die goedere en dienste wat soortgelyk is aan die goedere en dienste waarvoor die handelsmerk geregistreer is, sonder die handelsmerk-eienaar se toestemming, wat moontlik misleidend kan wees of verwarring veroorsaak.
3. 'n handelsmerkgebruik word, deurdat handel gedryf word met goedere en dienste wat soortgelyk is aan die goedere en dienste waarvoor die handelsmerk geregistreer is, as so 'n handelsmerk algemeen bekend is in Suid-Afrika en die gebruik van die merk moontlik voordeel sal kry of skadelik wees tot die kenmerkende karakter of aansien van die geregistreerde handelsmerk (Viljoen, Du Plessis & Vivier, 2001: 72).

Die Handelsmerk Wet maak ook voorsiening vir die beskerming van ongeregistreerde, algemeen bekende handelsmerke teen die ongemagtigde gebruik en reproduksie, nabootsing of vertaling van die merk, in terme van goedere en dienste wat identies of soortgelyk is aan die goedere en dienste waarvoor die handelsmerk bekend is, indien die gebruik moontlik misleiding of verwarring kan veroorsaak (Viljoen, Du Plessis & Vivier, 2001: 72).

Die verskillende dispute wat moontlik kan voortspruit uit handelsmerk en domeinnaam-konflikte is reeds in Hoofstuk 5 by 5.4.3 en 5.4.5 bespreek. Dispute kom veral voor omdat daar nie van die mense wat die registrasie behartig, vereis word om na te gaan of die betrokke naam reeds deur handelsmerke beskerm word nie ("Domeinname vir 'n makliker lewe", 2002:2).

6.5.2 Domeinnaam Owerheid (DNA)

Die Suid-Afrikaanse regering voel dit is belangrik dat alle mense wat domeinname registreer, bekwaam en in staat moet wees om die stelsel reg te administreer. Volgens die Departement

Stellenbosch University http://scholar.sun.ac.za

Kommunikasie het die onlangse situasie in Suid-Afrika vereis dat 'n nuwe bestuurstruktuur vir domeinname tot stand gebring word. Hiervoor het die Elektroniese Kommunikasie en Transaksies Wet van 2002 voorsiening gemaak deur die stigting van 'n onafhanklike Domeinnaam Owerheid (DNA- Domain Name Authority).

Die regering en Mike Lawrie, wat voorheen die za domeinnaam beheer het, het oor verskeie aangeleenthede gestry, soos oor wie die za-domein moet bestuur, met Lawrie wat aangevoer het dat die taak deur 'n onafhanklike liggaam beskerm moet word. Die Domeinnaam Owerheid sal die kwessie ten dele oplos deur 'n paneel saam te stel wat nie deur die regering verkies sal word nie, maar wel deur hom bekragtig word ("Domeinname vir 'n makliker lewe", 2002: 2).

In November 2002 het die Minister van Kommunikasie, dr. Ivy Matsepe-Casaburri, die paneel, wat volgens hoofstuk 10 van die Wet verantwoordelik sal wees vir die benoeming van 'n kortlys kenners vir die Domeinnaam Owerheid, bekendgemaak. Die lede van die paneel is: Sello Matsabu (voorsitter), Ryk Meiring, Mike Lawrie, Zodway Manase en Sebiletso Mokone Matabane. Aangesien Lawrie lid van die paneel is, mag hy nie ook in die owerheid dien nie. Die paneel het aansoeke vir die owerheid tot 15 Desember 2002 ontvang en beoordeel. Volgens Matsepe-Casaburri sal die proses teen Februarie 2003 voltooi wees (Kok, 2002: S7).

Die nie-winsgewinde organisasie sal na sake soos die voorsiening van universele Internet-adresse kyk en dispute oor handelsmerk-kuberplakkery oplos. Die liggaam gaan deur internasionale organisasies soos ICANN bemagtig word ("Domeinname vir 'n makliker lewe", 2002: 2).

6.5.3 Gevallestudie: SAL vs neverflysaa.com

Die Suid-Afrikaanse Lugdiens het op 9 April 2002 'n klag by die Nasionale Arbitrasie Forum gelê teen die domeinnaam www.neverflysaa.com. Die Amerikaner Vern Six het ná 'n onbevredigende SAL-vlug in 2002 na Suid-Afrika die domeinnaam www.neverflysaa.com by www.register.com geregistreer. Sedert die bestaan van die webwerf het dit al meer as 6,5 miljoen bladindrukke gehad en meer as 81 000 intekenare op sy poslys (Six, 2002). SAL het die saak teen neverflysaa.com op 31 Mei 2002 verloor.

Volgens die uitspraak deur die Nasionale Arbitrasie Forum in die VSA, het SAL aangevoer hy het "SAA" as 'n handelsmerk in Suid-Afrika en 21 ander lande geregistreer en het dié handelsmerk al in die VSA gebruik. SAL het gevoel die registrasie van die domeinnaam www.neverflysaa.com is verwarrend ooreenstemmend met die geregistreerde handelsmerk "SAA" se webwerf www.flysaa.com. SAL het bevestig dat die toevoeging van "never" tot flysaa.com nie tot voordeel van die SAL-domeinnaam strek nie. In vorige uitsprake deur WIPO (World Intellectual Property Organization) soos Vivendi Universal v. Sallen, waar die domeinnaam vivendiuniversalsucks.com

Stellenbosch University http://scholar.sun.ac.za

se registrasie gekanselleer is, is bevestig dat nie alle Internet-gebruikers moedertaal Engelssprekendes is nie en dus deur die toevoeging van "sucks" verwar kan word. SAL se prokereurs het verder aangevoer dat Engels slegs een van Suid-Afrika se elf amptelike landstale is en gevolglik is die domeinnaam www.neverflysaa.com verwarrend ("South African Airway (Pty.) Limited v. Vern Six", 2002: 6-9).

Die Nasionale Arbitrasie Forum het egter bevind dat Internet-gebruikers nie verwar sal word tussen die twee domeinname www.flysaa.com en www.neverflysaa.com nie ("South African Airway (Pty.) Limited v. Vern Six", 2002: 11).

Die gevallestudie bewys weer eens watter gevare en uitdagings die Internet vir handelsmerkhouers inhou (Muhlberg, 2002: 2).

6.6 Kubermisdaad

Met die Elektroniese Kommunikasie en Transaksies Wet van 2002 het Suid-Afrika vir die eerste keer voldoende wetgewing om kubermisdaad in die land te bekamp. Die verskillende soorte kubermisdaad - kuberkrakery, gevaarlike kodes, pakket-snuffel en gewone misdaad wat deur middel van rekenaarstelsels gepleeg word - is reeds in Hoofstuk 5 by 5.6 bespreek.

Vir enige persoon of onderneming wat inligting op rekenaardatabasisse of die Internet plaas, is die veiligheid van hul inligting en veral hul persoonlike besonderhede van die grootste belang. As dit by inligtingsekerheid kom, is daar vier belangrike doelstellings:

1. **Vertroulikheid:** die versekering dat inligting nie bekend gemaak sal word of aan ongemagtigde persone uitgereik word nie.
2. **Integriteit:** die versekering dat ongemagtigde skepping, verandering of vernieting van inligting verhoed word, om die konsekwentheid van inligting te verseker.
3. **Beskikbaarheid:** die versekering dat gemagtigde gebruikers nie toegang tot die inligting geweier word nie.
4. **Gemagtigde gebruik:** die versekering dat inligting nie op onwettige maniere of deur ongemagtigde mense gebruik word nie ("Sekerheid van groot belang vir sukses", 2002: 3).

Die risiko's wat verbonde is aan die Internet maak wetgewing om kubermisdaad te bekamp in enige land 'n noodsaaklikheid. Die Elektroniese Kommunikasie en Transaksies Wet van 2002 maak in hoofstuk 12 en 13 daarvoor voorsiening.

Die kuberinspekteurs wat in terme van hoofstuk 12 van die Wet deur die regering aangestel gaan word, gaan die kuberruim monitor vir kuberkrakers en mense wat bedrog pleeg. Die inspekteurs gaan by magte wees om fisieke en kuber gebiede te deursoek en kan op eiendom beslag

Stellenbosch University http://scholar.sun.ac.za

lê, afhangend of daar bevel in terme van seksie 83 (1) van die Wet uitgereik is. Diegene wat nie met die kuberinspekteurs saamwerk nie, of verhinder dat die kuberinspekteurs hul taak uitvoer, is skuldig aan 'n misdaad ("Electronic Communications and Transactions Act", 2002).

Die Elektroniese Kommunikasie en Transaksies Wet van 2002 bevat die eerste statutêre bepalings – onder Suid-Afrikaanse wetgewing – oor kubermisdaad. Die kubermisdade waarvoor in seksies 37(3), 40(2), 58(2), 80(5), 82(2) en 86(1)-(5) van die Wet voorsiening gemaak word, is, onder meer:

1. onwettige kriptografiese voorsieners
2. ongemagtigde toegang tot inligting
3. onderskepping of peutery met inligting
4. rekenaarverwante afpersing, bedrog en vervalsing ("Electronic Communications and Transactions Act", 2002).

Diegene wat skuldig bevind word aan dié kubermisdade kan tot vyf jaar in die tronk deurbring ("Electronic Communications and Transactions Act", 2002).

6.6.1 Gevallestudie: r00t3rs

In Oktober 2002 het die kuberkrakergroep r00t3s verwoesting onder Suid-Afrikaanse webwerwe gesaai. Die kuberkrakers wat tientalle Suid-Afrikaanse webwerwe verwoes het, het op webwerwe gefokus wat op die Windows NT-stelsel gebou is en het op 'n swak plek in die stelsel toegeslaan om toegang tot die webwerf te kry en dit dan heeltemal te verwoes.

Van die webruimtes wat verwoes is, sluit onder meer in: www.cluttons.co.za, www.pcjunction.co.za, www.avondalewine.co.za, www.vishuis.co.za, www.dowwedolla.co.za en www.signalhill.co.za.

Volgens Reinhardt Buys van Buys Inc. wat spesialiseer in e-handelsreg, het die groep elke keer op dieselfde wyse te werk gegaan. "Die bladsy-inhoud word heeltemal uitgewis en hy los in die meeste gevaal net sy naam in die hoek van 'n bladsy," het Buys in 'n onderhoud aan *Die Burger* gesê (Ferreira, 2002: 1).

Dié kuberkrakergroep is 'n groep 13-jarige Brasiliaanse seuns. Volgens Justin Stanford, 'n gerehabiliteerde kuberkraker en nou 'n direkteur van 4D Digital Security in Suid-Afrika, het hy ná 'n uitgebreide kuberspeurtog twee van die r00t3rs-groeplede in 'n kletskamer opgespoor waar hulle in Engels spog oor hul webwerf-verwoestingsveldtog.

Nie een van die lede van r00t3s kan aan Suid-Afrika uitgelewer word nie, omdat Brasilië nie Internet-wetgewing het wat dit onwettig maak om ander rekenaars uit Brasilië aan te val nie.

Stellenbosch University http://scholar.sun.ac.za

Al wat Suid-Afrikaners in so 'n geval sal help, is om te sorg dat hul rekenaars en inligtings-tegnologie-stelsels die jongste sekerheidsprogrammatuur bevat (Ferreira, 2002: 3).

'n Lys van kuberkrakery-gevalle wat sedert 2001 in Suid-Afrika plaasgevind het, verskyn in Bylae G.

6.7 Samevatting

Die Suid-Afrikaanse regstelsel is slegs van toepassings op dié dele van die Internet-ruggraat wat binne die Suid-Afrikaanse landsgrense val. Wanneer dit die Suid-Afrikaanse grense oorsteek, sal een van twee jurisdiksies van toepassing raak: die jusisdiksie van 'n ander land, of die jurisdiksie van internasionale wetgewing (Alberts, 2001: 398).

Die regulering van die ruggraat van die Internet in Suid-Afrika verskaf nie probleme nie, omdat dit by 'n reeds bestaande en doeltreffende stelsel inskakel, naamlik die reguleringstelsel van telekommunikasie in die land.

Die Elektroniese Kommunikasie en Transaksies Wetsontwerp wat aan die begin van 2002 vir kommentaar van belanghebbendes verskyn het, het 'n wankelrige pad gehad totdat dit later daardie jaar wet geword het (De Wet, 2002: 1). Die groot regtelike onsekerheid wat in Suid-Afrika geheers het, is met die verordening van die Elektroniese Kommunikasie en Transaksies Wet 25 van 2002 verwyder (Jansen, 2002: 2).

Ongekende magte word aan die Minister van Kommunikasie in hoofstuk 10, wat handel oor domeinnaamagentskappe en –administrasie, toegeken wat die beheer en administrasie van die .za domeinnaam aanbetref ("Comments on the ECT Bill by Namespace ZA", 2002: 5).

Meiring (2002) glo weer die regering se beheer oor die .za domein sal 'n degradasie in die huidige aanlyn-status van dié domein tot gevolg hê. Hy is ook bekommerd oor die gebrek aan deursigtigheid en verantwoordelikheid wat die lede van die voorgestelde agentskap sal hê (Meiring, 2002: 3).

Hoofstuk 11 is volgens Meiring (2002) 'n verligte benadering tot die kwellende vraag of Internet-diensverskaffers en ander bemiddelaars wetlik verantwoordelik gehou kan word vir die inligting wat hulle onwetend stoor en versend. Dit verskaf voldoende beskerming aan alle partye wat deur die potensiële verantwoordelikheid geraak word, wat uit die onwettige inhoud of kommunikasies na vore kan kom (Meiring, 2002: 9).

Die instelling van kuberinspekteurs soos in hoofstuk 12 van die Wet uiteengesit, se bedoeling is volgens Meiring (2002) prysenswaardig, maar hy glo die rol van polisiëring moet aan die Suid-Afrikaanse Polisie Diens oorgelaat word en dan in besonder die huidige Rekenaar Misdaad

Stellenbosch University http://scholar.sun.ac.za

Eenheid. Om 'n parallelle diens soos die kuberinspekteurs in te stel, wat nie 'n voldoende stelsel van wigte en teenwigte het nie, voorsien die Departement Kommunikasie van 'n ongeoorloofde uitbreiding van sy magte.

Meiring (2002) glo sekere dele van die Wetsontwerp se tekortkominge is van so 'n aard dat dit die gevaar loop om die aktiwiteite te onderdruk waarvoor die Wet ontwerp is. Ander is glo nagemaak en onnodig en plaas geweldige onkostes op die Suid-Afrikaanse ekonomie wat nie tot die regering of sy burgers se voordeel strek nie. Volgens Meiring is daar ander dele van die Wetsontwerp wat ingrypende en ongedefinieerde nuwe magte om na goeddunke te handel aan die Minister van Kommunikasie toeken. Dié nuwe magte word nie aan voldoende toesig en wigte en teenwigte onderwerp nie en is dus vatbaar vir misbruik (Meiring, 2002:14).

Dit is heeltemal begryplik dat Suid-Afrika die Afrika-kontinent in die uitreiking van elektroniese handel- en Internet verwante wetgewing sal lei. Daarom is dit belangrik dat die model wat Suid-Afrika voorstel en implementeer sonder enige verwyte is (Meiring, 2002: 17).

Suid-Afrika se Kopiereg Wet van 1978 is steeds van toepassing, ook op rekenaarprogramme, rekenaarnetwerke en die Internet.

Rekenaardatabasisse word beskerm as literêre werke. Internet webwerwe is gewoonlik multimedia produkte wat as literêre werke, kunstige werke, musikale werke en rekenaarprogramme beskerm word.

Die werking van die Kopiereg Wet is verleng deur 'n proklamasie in terme van seksie 37 na alle lande wat lede van die Bern Konvensie is wat in 'n bylae tot die proklamasie gelys is. Verwysings na die Suid-Afrikaanse Kopiereg Wet moet daarom in die lig daarvan geïnterpreteer word. Alhoewel die Bern Konvensie slegs van toepassing is op literêre en kunswerke is die proklamasie van toepassing op alle soorte werke wat in die Kopiereg Wet gedefinieer word (De Villiers, 2001: 42).

Tot en met die ingebruikneming van die Elektroniese Kommunikasies en Transaksies Wet van 2002 was Internet-diensverskaffers ook verantwoordelik gehou wanneer intekenare materiaal op hul webwerf geplaas het wat kopiereg skend. In terme van die Kopiereg Wet is 'n persoon wat 'n ander persoon veroorsaak of toestemming gee om sy Internet-diens te gebruik om kopieë van kopieregte werk te versprei, ook verantwoordelik vir die oortreding (De Villiers, 2001: 47).

Die Elektroniese Kommunikasie en Transaksies Wet van 2002 maak in Hoofstuk 11 egter voorsiening vir die beskerming van IDV's teen dié tipe van verantwoordelikheid van ander se oortredings ("Comments on the ECT Bill by Namespace ZA", 2002).

Stellenbosch University http://scholar.sun.ac.za

Die Handelsmerk Wet maak voorsiening vir die beskerming van geregistreerde en ongeregistreerde algemeen bekende handelsmerke teen die ongemagtigde gebruik en reproduksie, nabootsing of vertaling van die merk, in terme van goedere en dienste wat identies of soortgelyk is aan die goedere en dienste waarvoor die handelsmerk bekend is, indien die gebruik moontlik misleiding of verwarring kan veroorsaak (Viljoen, Du Plessis & Vivier, 2001: 72).

Die Suid-Afrikaanse regering voel dit is belangrik dat alle mense wat domeinname registreer, bekwaam en in staat moet wees om die stelsel reg te administreer. Volgens die Departement Kommunikasie het die onlangse situasie in Suid-Afrika vereis dat in terme van die Elektroniese Kommunikasie en Transaksies Wet van 2002 'n onafhanklike Domeinnaam Owerheid tot stand gebring word (DNA- Domain Name Authority).

Die nie-winsgewinde organisasie sal na sake soos die voorsiening van universele Internet-adresse kyk en dispute oor handelsmerk-kuberplakkery oplos. Die liggaam gaan deur internasionale organisasies soos ICANN bemagtig word ("Domeinname vir 'n makliker lewe", 2002).

Suid-Afrika het met die Elektroniese Kommunikasie en Transaksies Wet van 2002 vir die eerste keer voldoende wetgewing om kubermisdaad in die land te bekamp. Die Wet bevat die eerste statutêre bepalings – onder Suid-Afrikaanse wetgewing – oor kubermisdaad. Die kubermisdade waarvoor daar in seksies 37(3), 40(2), 58(2), 80(5), 82(2) en 86(1)-(5) van die Wet voorsiening gemaak word, is kuberkrakery, gevaarlike kodes, pakket-snuffel en gewone misdaad wat deur middel van rekenaarstelsels gepleeg word. Diegene wat skuldig bevind word aan dié kubermisdade kan tot vyf jaar in die tronk deurbring ("Electronic Communications and Transactions Act", 2002).

Die risiko's wat verbonde is aan die Internet maak wetgewing om kubermisdaad te bekamp in enige land 'n noodsaaklikheid.

In die volgende hoofstuk word die kernvraag van die studie beantwoord, naamlik of Internet-regulering in Suid-Afrika slegs deur die staat/regering behartig moet word en of dit moontlik is dat selfregulering en internasionale regulering van die Internet, staatsregulering kan vervang.

Stellenbosch University http://scholar.sun.ac.za

HOOFSTUK 7
GEVOLGTREKKING

In dié hoofstuk word die kernvraag van die studie beantwoord, naamlik of Internet-regulering in Suid-Afrika slegs deur die staat/regering behartig moet word en of dit moontlik is dat selfregulering en internasionale regulering van die Internet staatsregulering kan vervang. Die ooreenkomste en verskille tussen die gevolgtrekkings van dié studie en die literatuur wat in Hoofstuk 2 bespreek is, sal hier bestudeer word.

In Jason Niemczyk se studie (1999) *International Internet: A look inside* skryf hy die Internet se gebrek aan grense plaas 'n groot las op tradisioneel geografies gebaseerde regstelsels (Niemczyk, 1999:3).

Niemczyk se stelling is tot 'n mate waar, maar die regulering van die fisieke komponente van die Internet word deur 'n reeds bestaande geografies gebaseerde regstelsel, naamlik dié van telekommunikasie, gereguleer. Met die stigting van die Internasionale Telekommunikasie Unie het al die lande wat van telefoon-kommunikasie gebruik maak, hul ondersteuning gegee aan 'n internasionale regstelsel wat die skepping en implementering van universele en eenvormige telekommunikasie-standaarde regoor die wêreld fasiliteer (Alberts, 2001: 396).

Al wat dus "'n groot las op tradisioneel geografies gebaseerde regstelsels" plaas, is die inhoud van die Internet.

Die Internet het ontstaan uit die Amerikaanse Departement van Verdediging se skepping van ARPA (Advanced Research Projects Agency) (Cerf, 1993: 12). Toe was regulering nie 'n probleem nie, die Internet-gemeenskap was klein en maklik om sonder enige wetgewing te reguleer. Teen 1984 het die Internet vinniger en verder gegroei as wat ooit beplan is. Toe die publiek in 1991 aan die Wêreldwye Web (www) bekendgestel is, het dit baie gewild geraak en verder uitgebrei (Leiner, 2000: 19).

Die wyse waarop die Internet werk deur middel van hiperskakels, voorlopige berging, raamstelsels, spieël-webwerwe en die grenslose samestelling van die Internet, skep verskillende probleemareas vir kopiereg op die Internet.

Die voortbestaan van die Internet berus egter op webwerwe wat na ander webwerwe skakel, sonder die nodige toestemming. Daar word ook algemeen aanvaar dat die proses van voorlopige berging noodsaaklik is vir die doeltreffende gebruik van die Internet. Daarom is regulering wat die kwessies, betref redelik vaag (Viljoen, Du Plessis & Vivier, 2001: 71)

Stellenbosch University http://scholar.sun.ac.za

Vir enige onderneming is dit belangrik om dieselfde domeinnaam as hul handelsmerk te besit. Verskeie dispute het tussen diegene wat geen aanspraak op 'n domeinnaam het nie en die handelsmerkhouers wat wetlik daarop aanspraak kan maak, ontstaan. Terwyl daar 'n verskeidenheid identiese handelsmerke 'n gelyke bestaan voer as hulle gebruik en geregistreer is vir verskillende goedere en dienste of in verskillende gebiede, moet elke domeinnaam uniek wees. Van al die eienaars wat dieselfde handelsmerk besit, kan slegs een die ooreenstemmende domeinnaam registreer en gebruik.

Hier is dit weer eens die Internet se gebrek aan geografiese grense wat die hoofoorsaak van die probleem is. Wat dit erger maak is die feit dat die registrasie van enige domeinnaam wat nie presies identies aan 'n domeinnaam is wat reeds geregistreer is nie, wel toegelaat word (Viljoen, Du Plessis & Vivier, 2001: 74).

Die regulering van nasionale domeinname, soos .za, verskil van land tot land. Die Verenigde Nasies se WIPO en domeinnaam-registrateurs het reëls vir die TLD's ("top level domains"), maar daar is geen internasionale standaarde vir die domeine wat individuele lande verteenwoordig nie (Lyman, 2001:2).

Die grenslose omstandighede van die Internet is weereens die oorsaak van die probleme rondom jurisdiksie in die kuberruim. Die probleem raak egter erger wanneer 'n misdadiger in een land 'n Internet-verwante oortreding in 'n ander land begaan. Op die oomblik kan die misdadigers slegs onder die land waarin die oortreding plaasgevind het, se jurisdiksie geplaas word, as hy aan dié land uitgelewer word (Gordon, 2001: 441.442).

In 'n onlangse belangrike uitspraak aan die begin van 2003 het 'n Australiese hooggeregshof beslis dat beweerde laster wat in Amerika op die Internet gepleeg is, nou in Australië vervolg kan word. Oortreders van Internet-verwante misdade is voorheen gewoonlik in hul eie land aan die hand van plaaslike wetgewing vervolg (Rademeyer, 2003: 8).

Die feit dat daar nie een spesifieke organisasie, onderneming of regering is aan wie die Internet behoort nie, plaas 'n verdere las op die regulering, want niemand neem verantwoordelikheid nie (Hameed, 2002:3).

Dit is daarom dat regulering wat spesifiek vir die Internet ontwerp is, noodsaaklik is, aangesien bykans elke aspek van die reg deur die Internet uitgedaag word en baie regsraamwerke onvoldoende is om dit te hanteer (Opperman, 2000:5).

Suid-Afrika het dit ook besef en in 2002 is die land se Elektroniese Kommunikasie en Transaksies Wet van 2002 in werking gestel. Die wetsontwerp het baie reaksie uitgelok, sommige positief, ander negatief, maar al die belanghebbendes het saamgestem dat dit nodige wetgewing is wat al reeds te lank geneem het om te voltooi (Vegter & De Wet, 2002: 29-30).

Stellenbosch University http://scholar.sun.ac.za

Internasionale regstoepassing is nog meer kompleks, aangesien die meeste lande se vermoë om wetgewing toe te pas op 'n oortreding, wat as 'n misdaad onder hul wetgewing beskou word, beïnvloed word deur die bepaling van die *locus delicti*, die plek van oortreding. Misdade wat in een land plaasvind, kan nou deur middel van die Internet reg oor die wêreld plaasvind (Niemczyk, 1999 :11).

Suid-Afrika het duidelik van die probleem kennis geneem toe die jong Brasiliaanse kuberkrakergroep, r00t3s, verwoesting onder Suid-Afrikaanse webwerwe gesaai het en nie een van die lede aan Suid-Afrika uitgelewer kon word nie omdat Brasilië nie Internet-wetgewing het wat dit onwettig maak om ander rekenaars uit Brasilië aan te val nie. Al wat Suid-Afrikaners in so 'n geval sal help, is om te sorg dat hul rekenaars en inligtings-tegnologiestelsels die jongste sekerheidsprogrammatuur bevat (Ferreira, 2002: 3).

Die ander probleem met die huidige regulering van die Internet is dat intellektuele eiendomsregulering nasionaal gebaseerd is. Enigeen wat op die Internet publiseer, kan intellektuele eiendomsreg of enige ander regte of wette op enige plek in die wêreld oortree. Weens die aard van die Internet sal regerings daarom gedwing word om in die toekoms wetgewing te standaardiseer (De Villiers, 2000: 3).

Regerings is reeds besig om wetgewing in die verband te standaardiseer. Die intellektuele eiendomsveld in Suid-Afrika word op die oomblik deur verskeie internasionale konvensies en ooreenkomste gereguleer. Die ooreenkomste maak sommige regulering van die oortreding van intellektuele eiendomsreg oor grense moontlik deur die ondergetekendes te dwing om buitelandse werke deur die wysiging van hul plaaslike wetgewing te beskerm (De Villiers, 2001: 37-38).

'n Ander belangrike stap in die rigting van gestandaardiseerde wetgewing is die Europese Raad se internasionale Konvensie oor Kubermisdaad. Dis die eerste internasionale ooreenkoms oor misdade wat via die Internet en ander rekenaarnetwerke gepleeg word. Die hoofdoel van die konvensie is om 'n algemene misdaadvoorkomingsbeleid na te streef wat daarop gemik is om die gemeenskap teen kubermisdaad te beskerm deur veral internasionale samewerking aan te moedig ("Conventions on Cybercrime", 2001 :1).

'n Aantal inisiatiewe is van stapel gestuur om te sorg vir die standaardisering van die regulering van Internet soos onder meer ISOC se stigting van die IAHC (Internasionale Ad Hoc Komitee). IAHC het die privaatsektor-raamwerk gTLD-MoU ("Generic Top-Level Domain Memorandum of Understanding") geskep. Dit was die internasionale raamwerk waarbinne die administrasie en versterking van die Internet se DNS (Domeinnaam Stelsel) ontwikkel en uitgevoer is (Viljoen, Du Plessis & Vivier, 2001: 86).

Stellenbosch University http://scholar.sun.ac.za

Kuberplakkery word deur die tekort aan internasionale reëls bevorder (Lyman, 2001: 3). Volgens WIPO moet die internasionale gemeenskap begin saamstem oor watter regulering van toepassing is as hulle die groeiende probleem van kuberplakkery wil bekamp. WIPO glo die huidige regulering van die Internet DNS is heeltemal onvoldoende en 'n breër stel reëls moet ontwikkel word (McDonald, 2001: 1).

Die Internet-reguleringstudies wat in Hoofstuk 2 bespreek is, is die regulering wat tans vir die Internet beskikbaar is, wat uit selfregulering en die soewereine oplossing bestaan. Niemczyk se voorstel in sy studie *International Internet: A look inside* (1999) van 'n Internasionale Internet-regeringsliggaam is ook bespreek.

Selfregulering sluit strategieë soos self-help, kollektiewe aksie en private kontrakte in (Niemczyk, 1999). Volgens Niemczyk (1999) is die probleem met selfregulering die feit dat die reëls ontwikkel is toe die Internet nog jonk, en die aantal gebruikers min was. In so 'n omgewing was die selfreguleringsbenadering voldoende, omdat die Internet-gemeenskap 'n klein, intellektuele groep was, en nie die groot massas wat vandag die Internet gebruik nie. Die selfreguleringsmetode kan nie met miljoene gebruikers die Internet suksesvol reguleer nie.

Internet-gebruikers sal voortgaan om selfreguleringsmetodes te gebruik selfs al is daar voldoende wetgewing beskikbaar. In die M-Web Afrikaans vs watkykjy.co.za gevallestudie het M-Web Afrikaans van die selfreguleringsmetode gebruik gemaak om die situasie op te los. Die vorige bestuurder, Stefanie Hefer, van M-Web Afrikaans het in 'n volledige skriftelike antwoord aan watkykjy.co.za haar kant van die kant van die saak gestel. Haar brief is volledig op watkykjy.co.za gepubliseer met 'n verskoning van watkykjy.co.za aan Hefer (Hefer, 2003).

Die soewereine oplossing versterk nasionale regerings se regulering van die Internet deur huidige regstelsels, skep internasionale verdrae om verskille tussen nasionale regerings op te los en stel ooreenkomste in tussen die industrie en die regerings (Niemczyk, 1999: 8).

Die groot regtelike onsekerheid wat in Suid-Afrika geheers het, is met die verordening van die Elektroniese Kommunikasie en Transaksies Wet 25 van 2002 verwyder (Jansen, 2002). Volgens Ryk Meiring (2002) van die Information Technology Lawyers' Forum is sekere dele van die Wet se tekortkominge van so 'n aard dat dit die gevaar loop om die Wet te onderdruk (Meiring, 2002:1).

Regerings se reguleringsmag oor 'n individu word op jurisdiksie gebaseer. Jurisdiksie is grootliks afhanklik van ligging en teenwoordigheid (Niemczyk, 1999: 3). Niemczyk glo (1999) dié stelsel werk goed vir die regulering van aktiwiteite in die nie-Internetwêreld omdat dit op 'n geografiese model van teenwoordigheid gebaseer is.

Benewens die jurisdiksie-probleme wat nasionale regerings se regulering van die Internet skep, is meer en meer lande besig om wetgewing in te stel om die Internet te reguleer. Suid-Afrika se

Stellenbosch University http://scholar.sun.ac.za

Elektroniese Transaksies en Kommunikasies Wet 25 van 2002 het benewens geweldige reaksie uit die privaatsektor aan die einde van 2002 in werking getree (Vegter & De Wet, 2002: 29-30).

Die meeste kenners glo tegnologie self is die beste manier om kopiereg op die Internet te beskerm (Buys, 2001: 39). Dit is egter nie 'n voldoende reguleringsmeganisme nie, aangesien kuberkrakers daarvoor bekend is om deur die sekuriteitsmeganismes van dié tipe sagteware te breek.

Sedert die begin van die Internet in Suid-Afrika het die aantal rolspelers en organisasies in dié bedryf nie net tot die regering se regulerende rolspelers en organisasies beperk gebly nie. Daar is ook takke van internasionale Internet-organisasies wat in Suid-Afrika bedrywig is, maar ook belangrike onafhanklike nasionale Internet-organisasies en rolspelers wat die Internet in Suid-Afrika vorm deur hul interne regulering.

Weens die probleme wat die Internet skep om voldoende regulering moontlik te maak, glo Niemczyk (1999) 'n Internasionale Internet-reguleringsliggaam is 'n moontlike oplossing. Só 'n liggaam sal 'n stelsel van wigte en teenwigte bied, wat noodsaaklik is vir die doeltreffende regulering van 'n globale entiteit soos die Internet (Niemczyk, 1999).

Uit die gevolgtrekking van dié studie is dit duidelik dat Internet-regulering in Suid-Afrika nie slegs deur die regering behartig moet kan word nie. Suid-Afrika vorm reeds deel van verskeie lande wat aan internasionale konvensies van gestandaardiseerde regulering van die Internet deelgeneem het. Die fisieke struktuur van die Internet word deur die reeds gevestigde en aanvaarde regulering van die telekommunikasiebedryf behartig.

Slegs internasionale wetgewing soos Niemczyk se voorstel van 'n Internasionale Internet-reguleringsliggaam is ook nie voldoende nie, aangesien die wêreld se supermoondhede dié beleidsraamwerke en die skepping van reëls sal oorheers. Die "digitale gaping" wat reeds tussen ontwikkelde en minder onwikkelde lande heers, sal slegs groter word.

Die oplossing vir regulering van die Internet in Suid-Afrika wat uit die studie na vore kom is:

1. meer deelname aan internasionale konvensies wat die gestandaardiseerde regulering van die Internet bevorder;
2. minder ingrypende en ongedefinieerde nuwe magte om na goeddunke te handel wat aan die Minister van Kommunikasie gegee word, sonder 'n voldoende stelsel van wigte en teenwigte; en
3. Suid-Afrikaanse- en internasionale Internet-organisasies in Suid-Afrika moet deur die regering genader word om hulp te verleen met die regulering en adminstrasie van die Internet in Suid-Afrika.

Stellenbosch University http://scholar.sun.ac.za

Ongeag hoeveel Internet-regulerende liggame bestaan, hoeveel internasionale Konvensies oor die regulering van die Internet opgestel word en hoeveel regulerende wetgewing lande instel, word die Internet en die Wêreldwye Web deur individue vir hulself of hul werkgewers gebruik.

Individue moet hulle dus onderwerp aan sekere riglyne, regulasies en etiese kodes aangesien dit individue is wat aan die pen gaan ry. Daarom behoort, indien 'n individu enige webwerf of domein binnegaan, te weet hy onderwerp hom aan 'n stel riglyne, regulasies of etiese kode. Die meeste webwerwe het reeds riglyne, regulasies of etiese kodes waaraan gebruikers hul moet onderwerp, maar dit verskil van webwerf tot webwerf.

Daar behoort dus 'n uniforme Internet etiese kode te bestaan wat insluit van sosiale gedrag (netiket) tot wettiese voorskrifte en verpligte wat betref kopiereg, domeinname en handelsmerke en kubermisdaad.

Hier is 'n voorbeeld van hoe so 'n Etiese kode vir Internetgebruikers behoort te lyk:

- **Internet-gebruikers Etiese Kode:**

Die doel van dié Etiese kode is om 'n stel riglyne te verskaf waarvolgens alle Internet-gebruikers hul aktiwiteite op die Internet kan behartig en bepaal wat word as aanvaarbare gedrag op die Internet beskou.

Netiket:

- Jy, die gebruiker, moet jou verset teen alle vorme van diskriminasie, teistering en lasterlike uitlatings.
- As gebruiker van die Internet en Wêreldwye Web moet jy te alle tye eerlik en opreg wees.
- Die sosiale norme en waardes van ander Internet-gebruikers respekteer, maar nie ten koste van jou, as gebruiker, se eie sosiale norme en waardes nie.
- Jy, as gebruiker, moet jou privaatheid en die van ander individue respekteer.

Kopiereg:

- Alle inhoud, handelsmerke en data op webwerwe, insluitende maar nie beperk tot, sagteware, databasisse, teks, grafika, ikone, hiperskakels, private inligting en ontwerpe is die eiendom of gelisensieer tot die webwerf wat jy besoek en word sodoende beskerm teen skending deur plaaslike en internasionale wetgewing en verdrae.
- Webwerf-eienaars staan outomaties aan jou, die gebruiker, 'n persoonlike, nie-eksklusiewe lisensie toe vir die gebruik, uitdruk en tentoonstelling van al die inhoud, inligting,

Stellenbosch University http://scholar.sun.ac.za

sagteware, of leêrs op enige rekenaar, wat jy, die gebruiker, gebruik. Respekteer kopiereghouers se regte in terme van hul werke.

- Ongemagtigde kopiëring van inhoud, inligting, sagteware, of leêrs word verbied.
- Jy, die gebruiker, moet bewus wees van die wetgewing in jou land en die internasionale konvensies rakende kopiereg en kopiereg op die Internet. Veral konvensies waarvan jou land een van die ondergetekendes is, soos WIPO (World Intellectual Property Organization) se konvensie oor die beskerming van intellektuele eiendomsreg op die Internet.

Domeinname en handelsmerke:

- Jy, die gebruiker, sal onder geen omstandighede 'n domeinnaam registreer wat as kuberplakkery geklassifiseer kan word nie.
- Jy, die gebruiker, sal enige ongemagtigde registrasie van domeinname aan die betrokke domein-registrateur of enige domeindispuut-resolusie organisasie soos ICANN (The Internet Corporation for Assigned Names and Numbers) rapporteer.

Kubermisdaad:

- Jy, die gebruiker, word uitdruklik verbied om enige ongemagtigde toegang tot 'n webwerf te kry of probeer kry of om enige ongemagtigde, skadelike of kwaadwillige kode na 'n webwerf te stuur of te probeer stuur. Dit word deur plaaslike wetgewing en internasionale konvensies as 'n kriminele oortreding beskou.
- Jy, die gebruiker, sal jou nie skuldig maak aan enige van die volgende kubermisdade nie: Internet-bedrog (insluitend plagiaat), inligtingsdiefstal, kopieregskending, Internet-dobbelary en kinderpornografie.

Aangesien Internet-regulering van land tot land verskil, is dit die beste om jou aktiwiteite op die Internet volgens dié etiese kode en die onderskeie internasionale konvensies te behartig.

Stellenbosch University http://scholar.sun.ac.za

BYLAE A:
UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY

Stellenbosch University http://scholar.sun.ac.za

Uniform Domain Name Dispute Resolution Policy

Policy Adopted: August 26, 1999
Implementation Documents Approved: October 24, 1999

Notes:

1. This policy is now in effect. See www.icann.org/udrp/udrp-schedule.htm for the implementation schedule.

2. This policy has been adopted by all accredited domain-name registrars for domain names ending in .com, .net, and .org. It has also been adopted by certain managers of country-code top-level domains (e.g., .nu, .tv, .ws).

3. The policy is between the registrar (or other registration authority in the case of a country-code top-level domain) and its customer (the domain-name holder or registrant). Thus, the policy uses "we" and "our" to refer to the registrar and it uses "you" and "your" to refer to the domain-name holder.

Uniform Domain Name Dispute Resolution Policy

(As Approved by ICANN on October 24, 1999)

1. Purpose. This Uniform Domain Name Dispute Resolution Policy (the "Policy") has been adopted by the Internet Corporation for Assigned Names and Numbers ("ICANN"), is incorporated by reference into your Registration Agreement, and sets forth the terms and conditions in connection with a dispute between you and any party other than us (the registrar) over the registration and use of an Internet domain name registered by you. Proceedings under Paragraph 4 of this Policy will be conducted according to the Rules for Uniform Domain Name Dispute Resolution Policy (the "Rules of Procedure"), which are available at www.icann.org/udrp/udrp-rules-24oct99.htm, and the selected administrative-dispute-resolution service provider's supplemental rules.

2. Your Representations. By applying to register a domain name, or by asking us to maintain or renew a domain name registration, you hereby represent and warrant to us that (a) the statements that you made in your Registration Agreement are complete and accurate; (b) to your knowledge, the registration of the domain name will not infringe upon or otherwise violate the rights of any third party; (c) you are not registering the domain name for an unlawful purpose; and (d) you will not knowingly use the domain name in violation of any applicable laws or regulations. It is your responsibility to determine whether your domain name registration infringes or violates someone else's rights.

Stellenbosch University http://scholar.sun.ac.za

3. Cancellations, Transfers, and Changes. We will cancel, transfer or otherwise make changes to domain name registrations under the following circumstances:

a. subject to the provisions of Paragraph 8, our receipt of written or appropriate electronic instructions from you or your authorized agent to take such action;

b. our receipt of an order from a court or arbitral tribunal, in each case of competent jurisdiction, requiring such action; and/or

c. our receipt of a decision of an Administrative Panel requiring such action in any administrative proceeding to which you were a party and which was conducted under this Policy or a later version of this Policy adopted by ICANN. (See Paragraph 4(i) and (k) below.)

We may also cancel, transfer or otherwise make changes to a domain name registration in accordance with the terms of your Registration Agreement or other legal requirements.

4. Mandatory Administrative Proceeding.

This Paragraph sets forth the type of disputes for which you are required to submit to a mandatory administrative proceeding. These proceedings will be conducted before one of the administrative-dispute-resolution service providers listed at www.icann.org/udrp/approved-providers.htm (each, a "Provider").

a. Applicable Disputes. You are required to submit to a mandatory administrative proceeding in the event that a third party (a "complainant") asserts to the applicable Provider, in compliance with the Rules of Procedure, that

(i) your domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) you have no rights or legitimate interests in respect of the domain name; and

(iii) your domain name has been registered and is being used in bad faith.

In the administrative proceeding, the complainant must prove that each of these three elements are present.

b. Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of a domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the

Stellenbosch University http://scholar.sun.ac.za

trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location.

c. How to Demonstrate Your Rights to and Legitimate Interests in the Domain Name in Responding to a Complaint. When you receive a complaint, you should refer to Paragraph 5 of the Rules of Procedure in determining how your response should be prepared. Any of the following circumstances, in particular but without limitation, if found by the Panel to be proved based on its evaluation of all evidence presented, shall demonstrate your rights or legitimate interests to the domain name for purposes of Paragraph 4(a)(ii):

(i) before any notice to you of the dispute, your use of, or demonstrable preparations to use, the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have acquired no trademark or service mark rights; or

(iii) you are making a legitimate noncommercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

d. Selection of Provider. The complainant shall select the Provider from among those approved by ICANN by submitting the complaint to that Provider. The selected Provider will administer the proceeding, except in cases of consolidation as described in Paragraph 4(f).

e. Initiation of Proceeding and Process and Appointment of Administrative Panel. The Rules of Procedure state the process for initiating and conducting a proceeding and for appointing the panel that will decide the dispute (the "Administrative Panel").

Stellenbosch University http://scholar.sun.ac.za

f. Consolidation. In the event of multiple disputes between you and a complainant, either you or the complainant may petition to consolidate the disputes before a single Administrative Panel. This petition shall be made to the first Administrative Panel appointed to hear a pending dispute between the parties. This Administrative Panel may consolidate before it any or all such disputes in its sole discretion, provided that the disputes being consolidated are governed by this Policy or a later version of this Policy adopted by ICANN.

g. Fees. All fees charged by a Provider in connection with any dispute before an Administrative Panel pursuant to this Policy shall be paid by the complainant, except in cases where you elect to expand the Administrative Panel from one to three panelists as provided in Paragraph 5(b)(iv) of the Rules of Procedure, in which case all fees will be split evenly by you and the complainant.

h. Our Involvement in Administrative Proceedings. We do not, and will not, participate in the administration or conduct of any proceeding before an Administrative Panel. In addition, we will not be liable as a result of any decisions rendered by the Administrative Panel.

i. Remedies. The remedies available to a complainant pursuant to any proceeding before an Administrative Panel shall be limited to requiring the cancellation of your domain name or the transfer of your domain name registration to the complainant.

j. Notification and Publication. The Provider shall notify us of any decision made by an Administrative Panel with respect to a domain name you have registered with us. All decisions under this Policy will be published in full over the Internet, except when an Administrative Panel determines in an exceptional case to redact portions of its decision.

k. Availability of Court Proceedings. The mandatory administrative proceeding requirements set forth in Paragraph 4 shall not prevent either you or the complainant from submitting the dispute to a court of competent jurisdiction for independent resolution before such mandatory administrative proceeding is commenced or after such proceeding is concluded. If an Administrative Panel decides that your domain name registration should be canceled or transferred, we will wait ten (10) business days (as observed in the location of our principal office) after we are informed by the applicable Provider of the Administrative Panel's decision before implementing that decision. We will then implement the decision unless we have received from you during that ten (10) business day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that you have commenced a lawsuit against the complainant in a jurisdiction to which the complainant has submitted under Paragraph 3(b)(xiii) of the Rules of Procedure. (In general, that jurisdiction is either the location of our principal office or of your address as shown in our Whois database. See Paragraphs 1 and 3(b)(xiii) of the Rules of Procedure for details.) If we receive such documentation within the ten (10) business day period, we will not implement the Administrative Panel's decision, and we will take no further action, until we receive (i) evidence satisfactory to us of a resolution between the parties; (ii) evidence satisfactory to us that your lawsuit has been dismissed or

Stellenbosch University http://scholar.sun.ac.za

withdrawn; or (iii) a copy of an order from such court dismissing your lawsuit or ordering that you do not have the right to continue to use your domain name.

5. All Other Disputes and Litigation. All other disputes between you and any party other than us regarding your domain name registration that are not brought pursuant to the mandatory administrative proceeding provisions of Paragraph 4 shall be resolved between you and such other party through any court, arbitration or other proceeding that may be available.

6. Our Involvement in Disputes. We will not participate in any way in any dispute between you and any party other than us regarding the registration and use of your domain name. You shall not name us as a party or otherwise include us in any such proceeding. In the event that we are named as a party in any such proceeding, we reserve the right to raise any and all defenses deemed appropriate, and to take any other action necessary to defend ourselves.

7. Maintaining the Status Quo. We will not cancel, transfer, activate, deactivate, or otherwise change the status of any domain name registration under this Policy except as provided in Paragraph 3 above.

8. Transfers During a Dispute.

a. Transfers of a Domain Name to a New Holder. You may not transfer your domain name registration to another holder (i) during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded; or (ii) during a pending court proceeding or arbitration commenced regarding your domain name unless the party to whom the domain name registration is being transferred agrees, in writing, to be bound by the decision of the court or arbitrator. We reserve the right to cancel any transfer of a domain name registration to another holder that is made in violation of this subparagraph.

b. Changing Registrars. You may not transfer your domain name registration to another registrar during a pending administrative proceeding brought pursuant to Paragraph 4 or for a period of fifteen (15) business days (as observed in the location of our principal place of business) after such proceeding is concluded. You may transfer administration of your domain name registration to another registrar during a pending court action or arbitration, provided that the domain name you have registered with us shall continue to be subject to the proceedings commenced against you in accordance with the terms of this Policy. In the event that you transfer a domain name registration to us during the pendency of a court action or arbitration, such dispute shall remain subject to the domain name dispute policy of the registrar from which the domain name registration was transferred.

9. Policy Modifications. We reserve the right to modify this Policy at any time with the permission of ICANN. We will post our revised Policy at <URL> at least thirty (30) calendar days before it becomes effective. Unless this Policy has already been invoked by the submission of a complaint to a Provider, in which event the version of the Policy in effect at the time it was invoked will apply to you until the dispute is over, all such changes will be binding upon you with respect to any domain name

Stellenbosch University http://scholar.sun.ac.za

registration dispute, whether the dispute arose before, on or after the effective date of our change. In the event that you object to a change in this Policy, your sole remedy is to cancel your domain name registration with us, provided that you will not be entitled to a refund of any fees you paid to us. The revised Policy will apply to you until you cancel your domain name registration.

Comments concerning the layout, construction and functionality of this site should be sent to webmaster@icann.org.

Page Updated 17-May-2002

©2000, 2002 The Internet Corporation for Assigned Names and Numbers. All rights reserved.

Stellenbosch University http://scholar.sun.ac.za

BYLAE B:
CONVENTION ON CYBERCRIME

Stellenbosch University http://scholar.sun.ac.za

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

European Treaty Series - No. 185

CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Stellenbosch University http://scholar.sun.ac.za

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

c "service provider" means:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Stellenbosch University http://scholar.sun.ac.za

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Title 2 – Computer-related offences

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a any input, alteration, deletion or suppression of computer data;

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Title 3 – Content-related offences

Article 9 – Offences related to child pornography

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a producing child pornography for the purpose of its distribution through a computer system;

b offering or making available child pornography through a computer system;

c distributing or transmitting child pornography through a computer system;

d procuring child pornography through a computer system for oneself or for another person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a a minor engaged in sexually explicit conduct;

b a person appearing to be a minor engaged in sexually explicit conduct;

Stellenbosch University http://scholar.sun.ac.za

c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

a a power of representation of the legal person;

b an authority to take decisions on behalf of the legal person;

c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

Stellenbosch University http://scholar.sun.ac.za

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 – Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 3 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

Stellenbosch University http://scholar.sun.ac.za

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored

in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

Stellenbosch University http://scholar.sun.ac.za

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 – Jurisdiction

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

Stellenbosch University http://scholar.sun.ac.za

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

Stellenbosch University http://scholar.sun.ac.za

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

Stellenbosch University http://scholar.sun.ac.za

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

Stellenbosch University http://scholar.sun.ac.za

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV – Final provisions

Article 36 – Signature and entry into force

1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 – Accession to the Convention

1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Article 38 – Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:

- the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
- the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
- the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).

2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.

3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

Stellenbosch University http://scholar.sun.ac.za

Article 40 – Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

Article 41 – Federal clause

1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.

2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.

3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 – Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 – Status and withdrawal of reservations

1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.

2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.

3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).

Article 44 – Amendments

1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.

2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.

3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.

4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.

5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

Article 45 – Settlement of disputes

1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.

2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

Stellenbosch University http://scholar.sun.ac.za

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 – Denunciation

1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.

2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 – Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

a any signature;

b the deposit of any instrument of ratification, acceptance, approval or accession;

c any date of entry into force of this Convention in accordance with Articles 36 and 37;

d any declaration made under Article 40 or reservation made in accordance with Article 42;

e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

Stellenbosch University http://scholar.sun.ac.za

BYLAE C:
ISPA MEMBERS

Stellenbosch University http://scholar.sun.ac.za

ISPA
- About ISPA
- Members
- Membership Application
- Internet Exchange Points
- Regulatory
- Security Resources
- Development Initiatives
- Library
- FAQ's
- Legal Notice
- Members' Section

List of Members

The Internet Service Providers' Association (ISPA) currently has 56 members. If you are interested in joining the Association, please complete an application form .

Click on the ISP name below to open a window with a list of services on offer by that ISP. Information presented as supplied by ISPs.

Large Members

Company	Web site	Telephone number	E-mail address
AT & T Global Network Services SA	http://www.attbusiness.net	0800.117.888 +27.11.302.7260	direct@za.ibm.com
Connectit	http://www.connectit.co.za	0860.223.638	info@connectit.co.za
Data Pro Business Online	http://www.datapro.co.za	+27.11.809.1500 0800.111.304	info@datapro.co.za
Infosat	http://www.infosat.co.za	+27.11.721.3800	info@infosat.net
Internet Solutions	http://www.is.co.za	+27.11.283.5000	info@is.co.za
MTN Network Solutions	http://www.citec.net	+27.11.787.4251	info@citec.net
M-Web	http://www.mweb.co.za	+27.21.596.8300	sales@mweb.co.za
Posix Systems	http://www.posix.co.za	+27.12.807.0590	mje@posix.co.za
Storm Internet	http://www.stormnet.co.za	+27.11.202.3000	support@stormnet.co.za
Tiscali World Online	http://www.worldonline.co.za	+27.11.286.2600	candice.gibson@za.tiscali.com
UUNET (SA)	http://www.uunet.co.za	+27.21.658.8585	noc@za.uu.net

Medium Members

Company	Web site	Telephone number	E-mail address
Electronic Laboratory Services	http://www.elab.co.za	+27.11.358.0893	info@elab.co.za
eNetworks cc	http://www.enetworks.co.za	+27.21.421.9857	info@enetworks.co.za
Siemens Business Services	http://www.siemens.co.za	+27.11.652.2000	unicall@sbs.siemens.co.za

Small Members

Company	Web site	Telephone number	E-mail address
24-7 Internet Services	http://www.24-7.co.za	+27.11.789.7724	anthonye@24-7.co.za
AfriSat	http://www.afrisat.co.za	+27.13.755.4887	info@afrisat.co.za
Adept Internet	http://www.adept.co.za	+27.21.887.6262	info@adept.co.za
Artslink.co.za	http://www.artslink.co.za	+27.11.487.3689	info@artslink.co.za
AST Group	http://www.asta.co.za	+27.12.307.8902	johan.landman@ast.co.za
Bandwidth Barn	http://bandwidthbarn.org	+27.21.409.7000	alan@afridns.org
BCS-Net	http://www.bcsnet.co.za	+27.11.353.3228	hlee@bcsnet.co.za
Blue Sky Internet	http://www.digitalhost.co.za	+27.21.434.1201	info@digitalhost.co.za
Bucknet Internet	http://www.bucknet.co.za	086.110.1967	info@bucknet.co.za

Stellenbosch University http://scholar.sun.ac.za

East Coast Access	http://www.eastcoast.co.za	+27.31.566.8080	info@eastcoast.co.za
Imaginet Internet Services	http://www.imaginet.co.za	+27.46.622.3807	info@imaginet.co.za
Interexcel	http://www.interexcel.org	+27.12.346.1685	info@interexcel.co.za
Internet Shoppe	http://www.internetshoppe.co.za	+27.12.374.1549 +27.12.374.1907	cmc@ishoppe.co.za
Interprise	http://www.interprise.co.za	+27.11.803.4024	sandra@interprise.co.za
Intoweb Design	http://www.intoweb.co.za	+27.12.348.5320	darren@intoweb.co.za
Ion Access	http://www.ion.co.za	+27.31.204.8000	info@ion.co.za
iSpace	http://www.ispace.co.za	0860.477.477	administrator@ispace.co.za
Jantar ISP	http://www.jantar.co.za	+27.17.638.0137	janusz@jantar.co.za
Keyaka Weblink	http://www.kwl.co.za	+27.11.331.2660	info@kwl@co.za
MegaWeb Internet Services	http://www.megaweb.co.za	+27.11.485.1984	info@mega.co.za
MICS Online	http://www.mics.co.za	+27.12.661.9999	info@mics.co.za
NetConnect	http://www.netcon.co.za	+27.41.365.0465	adrian@netcon.co.za
Netline	http://www.netline.co.za	+27.11.248.2206	webmaster@netline.co.za
Netsurit	http://www.netsurit.com/nisp.htm	+27.11.444.3150	help@netsurit.com
Network & Computing Consultants	http://www.ncc.co.za	086.155.5444 +27.51.447.8589	vdm@ncc.co.za
NexGenCommunications	http://www.ngcom.co.za	+27.11.477.3604	info@ngcom.co.za
Obsidian Systems	http://www.obsisp.net/	+27.11.792.6500	info@obsisp.net
Oryx Trust	http://www.oryx.co.za	+27.42.296.0003	info@oryx.co.za
PCB Technologies	http://www.pcb.co.za	+27.11.487.3608	info@pcb.co.za
SANGONeT	http://www.sn.apc.org	0800.115.220 +27.11.838.6943	info@sn.apc.org
Satellite Data Networks	http://www.sdn.co.za	+27.11.535.7600	info@sdn.co.za
Sybaweb Internet	http://www.sybaweb.co.za	+27.21.683.3141	info@sybaweb.co.za
The S.A Internet	http://www.sai.co.za	+27.33.345.6777	wayne@sai.co.za
Uniforum	http://co.za	+27.11.314.0077	committee@uniforum.org.za
XM Solutions	http://www.xms.co.za	+27.11.444.2950	takis@xms.co.za
Xnet Internet Services cc	http://www.xnet.co.za	+27.11.867.5888	gary@xnet.co.za
ZAnet Internet Services	http://www.zanet.co.za	+27.11.465.0700	info@zanet.co.za
Zomerlust Systems Design	http://www.zsd.co.za	+27.21.683.1388	info@zsd.co.za

Affiliate Members

Company	Web site	Telephone number	E-mail address
CEQURUX Technologies	http://www.cequrux.com	+27.11.423.6065	info@cequrux.com
Concept Interactive	http://www.conceptinteractive.net	+27.21.448.8451	info@conceptinteractive.net
Host24.com	http://host24.com	+27.83.230.2481	johan@host24.com

Honorary Members

Company	Web site	Telephone number	E-mail address
Tenet	http://www.tenet.ac.za	+27.21.686.6010	ceo@tenet.ac.za
SchoolNet SA	http://www.school.za	+27.11.645.6400	info@school.za

Stellenbosch University http://scholar.sun.ac.za

BYLAE D:
CONSTITUTION OF THE INTERNET SERVICE PROVIDERS' ASSOCIATION

Stellenbosch University http://scholar.sun.ac.za

ISPA
About ISPA
Members
Membership Application
Internet Exchange Points
Regulatory
Security Resources
Development Initiatives
Library
FAQ's
Legal Notice
Members' Section

Constitution of the Internet Service Providers' Association

1. **Name**

1. The name of the association is the Internet Service Providers' Association.

2. "ISPA" is the official abbreviation for the Internet Service Providers' Association.

2.Interpretation

In this Constitution, "Internet access providers" shall mean persons that provide commercial Internet access.

3.Purpose

The ISPA is an independent body and voluntary association acting in the interests of Internet access providers in South Africa and generally dealing with matters related to the provision of Internet access in the Southern African region.

4.Mission

The ISPA's mission is to provide a non-profit forum in which Internet access providers can address issues of common interest and interface with industry stakeholders so that end?users receive world?class service and industry participants earn a fair return on their investments.

5.Mission Success Factors

The ISPA's mission success factors are:

1. To determine the needs of end?users in South Africa on an on?going basis;

2. To be a source and repository of relevant information for its members;

3. To influence industry regulation in South Africa concerning structures, policies, tariffs and competition;

4. To support and promote the implementation of regulated competition in the Internet access providers' industry;

5. To keep track of international communication trends;

6. To promote staff development and training in respect of its members; and

7. To extend Internet access to historically disadvantaged communities in South Africa.

6. Structure

Stellenbosch University http://scholar.sun.ac.za

1. The ISPA will consist of a general body of members involved in the provision of Internet access predominantly in South Africa.

2. The ISPA membership will elect a Management Committee to manage its day?to?day affairs.

3. The Management Committee may, from time to time and in its sole discretion, form and dissolve such sub?committees as it may deem fit to deal with specific matters of the ISPA, as contemplated in 15 below.

7. ISPA Membership

1. The membership of the ISPA shall consist of persons that provide Internet access in South Africa.

2. The Management Committee, may in their sole discretion, approve persons that provide Internet access in other countries, situated in the Southern African region, to join the ISPA as non-voting members.

3. All applications for membership must be made via the on? line ISPA membership application form housed on the ISPA Home Page at www.ispa.org.za, or by such other means as may be determined by the management Committee from time to time. No person will be admitted to be a member of the ISPA unless the Management Committee has approved his application for membership. The Management Committee shall be entitled, in their absolute discretion, to deny membership to any person who applies therefor in their sole discretion, provided that in such an event, such application may be approved by a majority of the members of the ISPA, subject to the provisions of 7.4 below.

4. The Management Committee may, in their sole discretion, revoke the membership of any member who fails to make full payment within 90 days of the due date for payment of membership fees.

5. The size of the ISPA will be restricted to such number of members, as may be determined by the management Committee from time to time in their sole discretion, which will ensure effective functioning of the ISPA.

6. A member's membership may be terminated by a majority vote of the members of the ISPA.

7. A member may terminate his membership of the ISPA at any time in writing to the management Committee.

8. Any member, whose membership of the ISPA has been terminated for whatsoever reason, shall forfeit all membership fees and other amounts paid by him to the ISPA.

8. Local Branches

1. The Management Committee may, in its sole discretion, authorise the establishment of a local branch of the ISPA in

Stellenbosch University http://scholar.sun.ac.za

any designated centre of South Africa.

2. A local branch shall be deemed established when the Management Committee approves the delegation of the powers of this Constitution to the centre in question.

3. Local branches shall act in accordance with general directions framed and adopted by the Management Committee and shall report to the Management Committee annually on their activities or within such other periods as the managing Committee may determine from time to time, which periods may be different in respect of different local branches.

9. Finances

1. Members will be required to pay such membership fees and by no later than such dates as may be determined by the Management Committee from time to time.

2. The Management Committee may, at its sole discretion, determine and institute different categories of membership and may prescribe different membership fees for such different categories. In this case, members will be equal members of the ISPA irrespective of any categorisation for the determination of fees, save to the extent that this Constitution provides otherwise or that the Management Committee determines otherwise at the time of creating such different categories.

3. Notwithstanding anything to the contrary contained herein, no member (or his representative) whose membership fees have not been paid on the due date therefor will be entitled to vote at any meeting of the ISPA or the Management Committee for as long as such membership fees remain outstanding.

4. Members will be responsible for all of their own expenses in connection with their membership of the ISPA. Exceptions to this rule require prior written Management Committee authorisation.

5. The Management Committee may accept unconditional offers from members or any other organisations to pay for special projects undertaken by the ISPA.

6. The Management Committee will be entitled to charge special levies to ISPA members from time to time to fund special projects of the ISPA which are necessary for or ancillary to the ISPA's mission as contemplated in 4 above, provided that such a special levy will have to be accepted by a majority of the ISPA membership as well.

10. Structure of the Management Committee

1. ISPA members will, annually during their annual general meeting, elect a Chairperson (or joint-Chairpersons), a Treasurer and one additional member to serve a twelve month term of office. These elected persons will form the Management Committee of the ISPA and shall all be natural persons.

Stellenbosch University http://scholar.sun.ac.za

2. The Management Committee will be entitled, but not obliged, from time to time to co-opt such additional members to the Management Committee to assist the Management Committee with specified projects. Such co-opted members shall not, for the purpose of this Constitution, be deemed to be members of the Management Committee.

3. In the case of the vacation for whatsoever reason of any of the positions of the management Committee prior to the appointment of a new Management Committee as aforesaid, a new office bearer will be elected by the majority of the members of the ISPA for the remainder of such term.

4. Upon a motion of no confidence in any office bearer supported by a majority vote of the members of the ISPA, such office bearer will be removed from his office and the provisions of 10.3 above shall apply.

5. The Management Committee shall hold not less than 1 (one) meeting during every two month period and may chose to hold additional meetings of the Management Committee, as and when necessary to the fulfilment of the Management Committee's duties.

6. If any Management Committee member has not been present in person or via a teleconferencing link at (3) three consecutive meetings, the position of that Management Committee member may be reviewed and, if deemed necessary, terminated by the majority of the remainder of the Management Committee.

11. Duties of the Management Committee

1. The primary duty of the Management Committee is to further the ISPA's mission, as specified in section 4 of this Constitution.

2. The Management Committee shall report on its activities and the affairs of the ISPA at all general meetings of the members of the ISPA.

3. The Chairperson(s) shall preside at all meetings at which he or she is present and shall enforce observance of the Constitution, sign minutes of meetings after confirmation, exercise supervision over the affairs of the ISPA and perform such duties as customarily pertain to the office of Chairperson.

4. Where two joint?Chairpersons have been elected, the Chairperson for any given meeting will be agreed beforehand and the member not occupying the chair will only have the rights accruing to a Management Committee member. In the event that no agreement on the foregoing can be reached, the majority of all other members present at such meeting will determine the chairperson of such meeting, which may not be any person other than one of the joint-Chairpersons.

5. The Treasurer shall be responsible to the members through the Management Committee for ensuring the

Stellenbosch University http://scholar.sun.ac.za

proper collection, administration and disbursement of the funds of the ISPA and that all legal and fiscal requirements are met.

6. The Management Committee shall appoint such persons, to act, on its behalf, as the Secretariat and Bookkeeper of the ISPA from time to time and to perform such functions and duties as are prescribed in this Constitution and as the Management Committee may from time to time determine, provided that these persons will not be required to be members of the ISPA and that, if they are not members of the ISPA, may be remunerated for their services as the Management Committee may determine.

7. Duties of the Secretariat shall include, inter alia:

    1. Receiving requests for meetings;
    2. Assuming responsibility for all ISPA correspondence;
    3. Keeping originals of letters received and copies of those dispatched;
    4. Attending all meetings, recording minutes of the proceedings and distributing such minutes to all members of the ISPA; and
    5. Keeping a register of all members and associated information.

8. Duties of the Bookkeeper shall include, inter alia:

    1. Maintaining the ISPA's accounts in such bank accounts as may be approved by the Management Committee from time to time;
    2. Ensuring that all financial information of the ISPA is available at meetings for discussion and approval; and
    3. Tabling a financial statement of the year's transactions at each Annual General Meeting for approval by the membership.

9. Prior to any Annual General Meeting, the Management Committee shall appoint a person or organisation to audit the financial statement, which is to be tabled thereat.

12. Powers of the Management Committee

1. In addition to anything contained in this Constitution and subject to the limitations stipulated in paragraph 12.3, the Management Committee shall be entitled to incur expenditure in the furtherance of its duties and take action in all matters on behalf of the ISPA.

2. The Management Committee is empowered to:

    1. Administer the assets of the ISPA generally;
    2. Open and close accounts at registered commercial banks in South Africa on behalf of the ISPA;
    3. Issue press statements on behalf of the ISPA;
    4. Approve or decline ISPA membership applications (as specified in 7.2 above);
    5. Revoke ISPA membership (as specified in 7.3 above);
    6. Authorise and oversee the establishment of local

Stellenbosch University http://scholar.sun.ac.za

branches of the ISPA (as specified in 8 above);
7. Call special general meetings (as specified in 14 below); and
8. Appoint sub-committees from time to time (as contemplated in 15 below).

3. The powers of the Management Committee shall be limited to the extent that it must seek the approval of the ISPA membership before:

    1. Determining ISPA membership fees (as specified in 9.1 and 9.2 above);
    2. Entering into any contracts other than in the ordinary course of performing its duties in terms hereof;
    3. Undertaking business transactions where the total amount of the transaction exceeds the ISPA's income during the previous three months.

13. General Meetings of Members of the ISPA

1. There will be not less than one ISPA meeting during any three-month period.

2. A quorum for meetings shall be one third of all members of the ISPA, present in person or via a videoconferencing link; or ten members, whichever is the smaller number.

3. Each ISPA member shall have one vote at each meeting.

4. All meetings will be open to all members and to any other interested observer at the discretion of the Management Committee.

14. Annual and Special General Meetings

1. There shall be 1 (one) annual general meeting not less than once every calendar year, which meeting will be held not less than 10 (ten) months after and not more than 14 (fourteen) months after the previous annual general meeting, and members of the ISPA will be given at least 21 (twenty one) days' notice thereof.

2. The Management Committee may call a special general meeting at any time, provided that at least 14 days' notice of any special general meeting is given to ISPA members.

3. The provisions of 13.2 to 13.4 above, both inclusive shall apply mutatis mutandis.

15. Sub-Committees

1. Sub-committees may be formed by the Management Committee in their sole discretion from time to time to deal with specific issues in accordance with a statement of objectives, as determined by the management Committee.

2. Each sub-committee must have a chairperson, which will be appointed by the Management Committee.

3. Minutes of each sub-committee meeting must be submitted

Stellenbosch University http://scholar.sun.ac.za

to Management Committee within fourteen days of the meeting.

4. The statement of objectives of each sub-committee, as well as its minutes must be made available by the chairperson of such sub-committee to any ISPA member on request, provided that such member shall bear all expenses in respect of such request.

5. Members of the Management Committee will be ex officio members of any such sub-committee.

16. Legal Personality

1. The ISPA shall be a juristic person capable of acquiring rights, incurring obligations, entering into legal transactions and of suing and being sued in its own name.

2. Immovable property acquired by the ISPA shall be registered in the name of the ISPA.

17. Accounting

1. The ISPA shall not distribute any of its profits or gains to any person and shall utilise its funds for the objects for which it has been established.

2. All moneys received on behalf of the ISPA shall be deposited in one or more accounts as contemplated in 12.2.2 above. All payments to be made on behalf of the ISPA shall be made by cheque drawn on any such account or by cheques issued by the commercial bank with which a particular account is operated.

3. Deposits into any such account may be made on the signature of any one Management Committee member, but all other operations on any such account shall be upon the signatures of two members of the Management Committee.

4. Proper books of the accounts of the ISPA will be kept as contemplated herein before. Such books, together with all other papers and documents connected with or relating to the ISPA, shall be kept at such place as may be determined from time to time by the Management Committee and must be accessible to each of the members of the ISPA.

18. Indemnity

1. Each member of the ISPA is indemnified out of and from the funds and property of the ISPA, against all losses, charges, costs, damages and other liability which that member may suffer or incur as a result of executing his duties as a member of the ISPA, save to the extent that such member acted negligently or fraudulently.

2. No member of the ISPA shall be answerable or deemed to be in any way responsible for any act or default of any other member or for any deficiency or insufficiency of any title or security whatsoever taken by the ISPA, save to the

Stellenbosch University http://scholar.sun.ac.za

extent that such member acted negligently or fraudulently.

3. No member of the ISPA shall be liable for any losses occasioned by the commercial bank or other persons with whom monies or securities of the ISPA are deposited or entrusted for safe custody, investment or otherwise, nor for any loss, misfortune or damage which may happen or take place in the execution of that member's duties or as a result thereof ISPA, save to the extent that such member acted negligently or fraudulently.

19. Dissolution

1. The ISPA shall be dissolved upon a resolution to that effect by two?thirds of the members at a general meeting or at a special general meeting convened for that purpose provided that notice of the proposed resolution is given to members not less than 14 days before the date of the meeting.

2. Upon the dissolution of the ISPA, the Management Committee shall, after making provision for the costs of dissolving the ISPA, distribute the accumulated funds of the ISPA to an Association not for Gain with similar objectives to those of the ISPA, as may be determined by the Management Committee in its sole discretion.

20. Alteration of the Constitution

This Constitution or any part thereof may be altered by a resolution passed by not less than 75% (seventy five percent) of ISPA members present at a general meeting or a special meeting convened for this purpose, provided that at least 14 (fourteen) days' notice of such special meeting is given to members.

21. Miscellaneous

1. The ISPA may not be used by any representative, liaison body or industry sector to further its own business interests, outside the objectives of the ISPA.

2. The ISPA address lists may not be used for any purpose other than the business of the ISPA, unless with the prior approval of the management Committee.

3. No action may be taken against a member or a member's representative, unless a report was tabled to the Management Committee and reasonable opportunity was given to the member or the member's representative to defend such member's position.

22. Language

The ISPA shall conduct business in any of the official languages of the Republic of South Africa. In the event of conflict, the English text of this Constitution shall take precedence over any translation thereof.

Stellenbosch University http://scholar.sun.ac.za

BYLAE E:
THE CONSTITUTION OF THE SOUTH AFRICAN CHAPTER OF THE INTERNET SOCIETY

Stellenbosch University http://scholar.sun.ac.za

THE CONSTITUTION

of the

SOUTH AFRICAN CHAPTER

of the

INTERNET SOCIETY

TABLE OF CONTENTS

Stellenbosch University http://scholar.sun.ac.za

THE CONSTITUTION

of the

SOUTH AFRICAN CHAPTER OF THE INTERNET SOCIETY

1. **PREAMBLE**

a. The persons reflected in the schedule attached hereto marked as annexure A wish to form ISOC-ZA as the South African chapter of ISOC and as a voluntary association not for gain.

a. Notwithstanding ISOC-ZA's affiliation with ISOC, the existence of ISOC-ZA shall be determined in accordance with South African law and the provisions of this constitution.

1. **NAME OF ASSOCIATION**

The name of the association is the South African Chapter of the Internet Society and the recognised abbreviation thereof shall be ISOC-ZA.

1. **DEFINITIONS**

a. In the interpretation of this constitution and unless the subject or context otherwise requires -

i. the following words and expressions shall have the following meanings -

(1) "authorised representative" - a person authorised, in the manner prescribed by the Act, to act as the representative of a company or other body corporate at a general meeting of ISOC-ZA;

(1) "executive committee" - the executive committee elected by the members in terms of clause 10

Stellenbosch University http://scholar.sun.ac.za

(1) "full members" - members of ISOC-ZA who are also members of ISOC;

(1) "individual members" - natural persons and created entities who qualify for individual membership of ISOC, whether as a regular individual member or a student member;

(1) "ISOC" - the Internet Society, a corporation incorporated as a non-profit corporation (without capital stock) in terms of the District of Columbia Non-Profit Corporation Act of the United States of America, being an international organisation for global co-operation in and co-ordination of the Internet and its internetworking technologies and applications;

(1) "ISOC-ZA" - the South African chapter of ISOC;

(1) "member" - any member of ISOC-ZA, initially being the persons referred to in annexure A and thereafter including any person whose membership has been approved by ISOC-ZA;

(1) "ordinary resolution" - a resolution approved by a simple majority of members present at a general meeting of members at which a quorum is present and of which notice has been given in accordance with clause 15.4;

(1) "organisational members" - organisations who are admitted as organisational members of ISOC and who contribute such supplementary organisational membership fees to ISOC-ZA as it may determine from time to time;

(1) "RSA" - the Republic of South Africa;

(1) "special resolution" - a resolution approved by not less than 75% of the members present at a general meeting

of members of which not less than twenty-one days' advance notice has been given and at which a quorum is present;

i. any gender includes the other genders;

i. a natural person includes a created entity and vice versa;

i. the singular includes the plural and vice versa;

i. when any number of days is prescribed such number shall exclude the first and include the last day unless the last day falls on a Saturday, Sunday or public holiday in the Republic of South Africa, in which case the last day shall be the next succeeding day which is not a Saturday, Sunday or public holiday in the Republic of South Africa.

i. any word or phrase defined in the body of this constitution as opposed to in clause 3.1.1 shall have the meaning assigned to it in such definition throughout this agreement.

1. **LEGAL PERSONA**

a. ISOC-ZA shall be a body corporate, independent of any individual member and shall be capable of contracting in its own name, owning and holding property (movable, immovable, corporeal or incorporeal) in its own name, and of suing or being sued in its own name.

a. No member of ISOC-ZA shall be liable in any way for any loss or damage that may be suffered by ISOC-ZA through any act or omission of that member or of any other member or by ISOC-ZA or by any of its servants or agents in the execution of any duty, unless such loss or damage is the result of that member's negligence or fraud.

Stellenbosch University http://scholar.sun.ac.za

a. No member shall have the right to or interest in any of the property or funds of ISOC-ZA.

a. ISOC-ZA shall apply its surplus income in promoting its objectives and shall not, at any time, make any distribution or pay any dividend or surplus to any of its members.

1. **REGISTERED ADDRESS**

The registered address of ISOC-ZA shall be as determined by the executive committee from time to time, initially being [ ] and the electronic mail address of ISOC-ZA shall be [ ]. Additional electronic addresses may be utilised by ISOC-ZA from time to time for various purposes, provided that unless notified to the contrary, the aforementioned electronic mail address shall be the only electronic mail address competent for the giving of notice to ISOC-ZA in terms of this constitution.

1. **PURPOSE**

a. ISOC-ZA shall be constituted as an association not for gain and the purpose of ISOC-ZA shall be to serve the interests of the South African segment of the global Internet community.

a. In fulfilling the purpose referred to in clause 6.1, ISOC-ZA shall serve all persons and entities who are resident, domiciled, employed, registered, or which conducts business, in the RSA or who are interested or involved in the South African Internet community.

a. ISOC-ZA shall be broadly inclusive on a regional, linguistic and racial basis and the community whose interests it shall serve shall be construed as widely as possible and shall include persons and entities who are connected to the Internet, as well as those who are not so connected but have an interest in the Internet.

a. ISOC-ZA shall be constituted as a chapter of ISOC. This constitution neither supersedes nor abrogates any of the by-laws of ISOC insofar as they regulate the affairs of regional chapter. Similarly the by-laws of ISOC regulating regional chapter affairs, as

may be amended from time to time, shall neither supersede nor abrogate any of the provisions of this constitution, unless agreed to and adopted by the members as provided for herein.

a. Without derogating from the generality of the purpose referred to in clause 6.1, the objectives of ISOC-ZA shall be to -

i. promote co-operation and dialogue between itself as a representative of the South African Internet community, Internet Service Providers, regulatory authorities and other interested parties;

i. act as a spokesperson for and representative of the South African Internet community on all matters;

i. regulate participation in and/or sponsorship of congresses, seminars and workshops;

i. do all such things as are incidental or conducive to the interests of the members and the South African Internet community or to the attainment of the purposes set out in this constitution.

1. **MEMBERSHIP**

a. The initial members of ISOC-ZA shall be the persons reflected as such in annexure A hereto.

a. ISOC-ZA shall initially have two classes of members, being organisational members and individual members both of which shall be classes of full membership. The members shall be entitled, by special resolution, to create additional classes of membership and/or vary the terms and conditions of the existing classes of membership.

a. Members of ISOC-ZA shall also be members of ISOC, provided that membership of ISOC or ISOC-ZA shall not be necessary for participation in the activities of ISOC or ISOC-ZA, however, no person or entity other than a member shall be entitled to vote at any

Stellenbosch University http://scholar.sun.ac.za

meeting of ISOC-ZA, other than by reason of a proxy given in terms of clause 17.

a. All individuals and organisations falling within the defined scope of ISOC-ZA as set out in this constitution shall, subject to clause 7.6, be eligible for membership without discrimination, other than for just cause.

a. Membership of ISOC-ZA shall be open to all members of ISOC in the RSA, upon request by such ISOC members and upon payment of all and any ISOC-ZA membership fees as may be determined from time to time.

a. If a person -

i. applies for membership of ISOC-ZA in the form prescribed by ISOC-ZA, which form shall include an undertaking by the applicant to be bound by the provisions of this constitution and the rules of ISOC-ZA;

i. pays to ISOC-ZA the relevant membership fee prescribed by the executive committee for the time being;

i. supports the objects of ISOC-ZA; and

i. complies with any further admission criteria laid down by the executive committee from time to time, which criteria shall not be discriminatory other than for just cause,

then such person shall be admitted as a member of ISOC-ZA.

a. In admitting a person as a member of ISOC-ZA, such person may be admitted as -

i. an individual member of ISOC-ZA; or

i. an organisational member of ISOC-ZA; or

i. a member in such other class of membership as may be created by ISOC-ZA from time to time.

a. Each member shall be bound by the provisions of this constitution and shall have all the rights given to it by this constitution and perform all of its obligations arising out of this constitution.

a. Any member may terminate its membership of ISOC-ZA by giving ISOC-ZA notice of its intention to do so; provided that the termination of membership shall not affect the liability of any member for full membership fees for the year in which such termination of membership occurs, or for any other amount due to ISOC-ZA and arising out of its activities for any period prior to the date on which its membership terminates.

a. The executive committee shall have the right to suspend or terminate the membership of any member which has -

i. not complied with the provisions of this constitution; or

i. failed to pay its membership fees or any other amount due to ISOC-ZA within three months of the due date or within such further period as may be determined by the executive committee at its discretion; or

i. breached any of the rules referred to in clause 29,

provided that the member concerned shall be given notice of the meeting of the executive committee at which its membership will be considered and allowed an opportunity of giving, orally or in writing, any explanation and defence the member thinks fit; provided further that a member whose membership has been suspended or terminated in terms hereof may, on notice in terms of clause 28, propose a special resolution at the next general meeting of ISOC-ZA overturning the decision of the executive committee to suspend or terminate its membership.

a. If any decision to suspend or terminate the membership of a member is made and such member disputes the correctness of

Stellenbosch University http://scholar.sun.ac.za

that decision, it shall, within thirty days of the decision being challenged, be referred for determination in accordance with 33.

a. A member shall cease to be a member immediately -

i. in the case of a natural person -

(1) on such member's death;

(1) if such member becomes a lunatic or of unsound mind;

(1) if such member's estate is surrendered or sequestrated, whether voluntarily or compulsorily;

i. in the case of a member which is not a natural person, if such member is liquidated, wound up or placed under judicial management, whether provisionally or finally and whether compulsorily or voluntarily.

a. Unless this constitution specifically requires that a special resolution be passed in order to exercise the powers of the members in general meeting, all of the powers of the members in general meeting may be exercised by ordinary resolution.

1. **OFFICERS**

a. ISOC-ZA shall have four officers, being the chairperson, vice-chairperson, secretary and treasurer. No person may hold more than one office simultaneously.

a. The officers of ISOC-ZA shall be elected at the annual general meeting of ISOC-ZA and serve for a period of twelve calendar months from 1 September of the year of their election until 30 August of the following year, provided that if the annual general meeting has not taken place prior to 30 August of any year, the period of office of the officers shall be extended until the date of the annual general meeting.

a. No individual shall serve for more than two consecutive years in any specific office provided that the provision of this clause 8.3 shall not preclude any individual from serving for more than two consecutive years as an officer of ISOC-ZA in a different office.

a. Should there be a vacancy in the officers of ISOC-ZA for any reason, such vacancy shall be filled by the executive committee co-opting a member or the authorised representative of a member (who need not be a member of the executive committee) to fill such vacancy; provided that such co-opted officer shall be subject to confirmation at the first general meeting of ISOC-ZA that is held after such co-option has taken place. Should the co-option of such officer not be confirmed at such general meeting, such general meeting shall elect a new officer to fill the vacancy.

a. The election of the officers shall take place at the annual general meeting at which the election of the executive committee takes place and the same provisions relating to the voting procedure and the election of the executive committee shall apply to the election of the officers, and in particular such voting procedure shall make provision for voting by electronic means.

1. **DUTIES OF OFFICERS**

a. **Chairperson**

The chairperson shall be the principle officer of ISOC-ZA and shall be responsible for leading ISOC-ZA and managing its activities in accordance with the policies and procedures of ISOC-ZA and this constitution. The chairperson shall preside at all meetings of ISOC-ZA and of the executive committee.

a. **Vice-chairperson**

The vice-chairperson shall preside at meetings of ISOC-ZA and the executive committee in the absence of the chairperson and shall generally assist the chairperson in the execution of the duties of such office.

Stellenbosch University http://scholar.sun.ac.za

a. **Secretary**

The secretary shall keep the minutes of all general meetings, executive committee meetings and any other meetings of ISOC-ZA. In addition the secretary shall -

i. in conjunction with the executive committee, prepare an annual report for presentation to ISOC-ZA at the annual general meeting;

i. prepare the ISOC-ZA activity report for submission to ISOC;

i. notify ISOC of any changes to the officers of ISOC-ZA; and

i. liaise with the ISOC Vice-President of Chapters with regard to any amendment to this constitution in accordance with clause 31 hereof.

a. **Treasurer**

The treasurer shall collect membership fees and all other amounts from creditors of ISOC-ZA, pay the debts of ISOC-ZA, maintain the financial records of ISOC-ZA and generally be responsible for the financial control and management of ISOC-ZA. In addition the treasurer shall -

i. prepare the interim ISOC-ZA annual financial report for presentation to the annual general meeting; and

i. prepare and submit the annual financial report to ISOC.

1. **EXECUTIVE COMMITTEE**

a. The executive committee shall act as an extension and representation of the general meeting and shall, in terms of clause 11, implement the broad policy directives passed by the members in general meeting.

a. The executive committee shall consist of eight members who shall be composed of -

i. the officers;

i. the immediately preceding chairperson. Provided that if the immediately preceding chairperson has ceased to be a member in terms of clause 7, has been re-elected as an officer, ceased to be a member of the executive committee in terms of clause 18.2.5 or is not prepared to act (collectively referred to as "declined") then the immediately preceding vice-chairperson shall be appointed to the executive committee and if the immediately preceding vice-chairperson has declined then the immediately preceding secretary shall be appointed to the executive committee and if the immediately preceding secretary has declined then the immediately preceding treasurer shall be appointed to the executive committee. Provided further that should all of the immediately preceding officers have declined (as shall be the case in respect of the first executive committee to be elected) then the members shall elect an additional member of the executive committee to fill such position;

i. the chairperson of three of the standing committees,

who shall be elected at the annual general meeting in accordance with the provisions of this constitution and mutatis mutandis on the same basis set out in clause 8.2.

a. Each officer and each chairperson of each of the standing committees shall be nominated and elected, in accordance with the provisions of this constitution, for the specific position which he or she is to hold.

b. The chairperson shall not have a casting vote at any meeting of the executive committee, the officers or any general meeting.

Stellenbosch University http://scholar.sun.ac.za

a. No member of the executive committee shall be entitled to any remuneration in respect of any service/s rendered by that member in his or her capacity as a member of the executive committee.

1. **POWERS AND DUTIES OF THE EXECUTIVE COMMITTEE**

Apart from the powers and duties mentioned in any other provision, the executive committee shall also have the following additional powers and duties -

a. to convene general meetings in terms of clause 15;

a. to do whatever is necessary to manage ISOC-ZA and to promote the purpose and objectives of ISOC-ZA;

a. to keep a register of the members of the executive committee and to record an address for each executive committee member;

a. to submit in conjunction with the secretary, annually, a report to the annual general meeting of ISOC-ZA dealing with the activities of ISOC-ZA during the preceding financial year and cause a copy of the report to be made available;

a. to appoint representatives to meet with any person, organisation, corporation and any other entity;

a. to manage the day to day affairs of ISOC-ZA in the best interests of its members;

a. to carry out and adhere to all resolutions passed by the members in general meeting;

a. to determine the manner in which applications for membership of ISOC-ZA by new members shall be submitted to it;

a. to consider applications for new membership of ISOC-ZA;

a. to recommend the annual membership fees to be paid by members from time to time including the membership fees in respect of different classes of membership;

a. to make recommendations regarding the appointment of an auditor or auditors;

a. to invest all monies of ISOC-ZA which are not required to meet current charges upon ISOC-ZA subject to the provisions of clause 19.2.6;

a. to defend, institute, abandon or compromise any action or proceedings in any court of law or other tribunal, by or against ISOC-ZA, which concerns the affairs of ISOC-ZA, but only after obtaining the prior approval (or subsequent ratification if the exigency of such legal proceedings precludes obtaining prior approval) of the members in general meeting to do so;

a. to obtain legal opinions in respect of any of the matters relating to the affairs of ISOC-ZA;

a. to make rules and regulations relating to its own activities.

1. **STANDING COMMITTEES**

a. ISOC-ZA shall have no less than three permanent standing committees and the three initial standing committees shall be the -

i. logistics standing committee;

i. education standing committee; and

i. membership and publicity standing committee.

Stellenbosch University http://scholar.sun.ac.za

a. The members, in general meeting, shall be entitled to vary the number and the areas of responsibility of the standing committees from time to time, provided that the number of standing committees shall not fall below three and the chairperson of no more than three of the standing committees, for the time being, shall also be members of the executive committee.

a. The chairperson of each of the standing committees shall be elected at the annual general meeting in accordance with this constitution. To the extent that there are more than three standing committees, in addition to the election of the chairperson of each standing committee, the annual general meeting shall, by way of a separate ballot, elect the chairperson of three of the standing committees already so elected as members of the executive committee.

a. Each of the standing committees shall be entitled to make rules and regulations relating to its own activities and with regard to the conduct of meetings thereof, provided that such rules and regulations shall not be inconsistent with the provisions of this constitution.

a. The chairperson of any standing committee shall not have a casting vote at any meeting of such standing committee.

1. **TEMPORARY COMMITTEES**

a. The executive committee shall be entitled to constitute such number of temporary committees as may be required from time to time. Any member may request the executive committee to constitute a temporary committee, which request shall specify the purpose for which such temporary committee will be formed and the members who will constitute such temporary committee. The consent of the executive committee to the formation of such temporary committee shall be required, which consent shall not be unreasonably withheld and the proposal for the establishment of a temporary committee shall be ratified, unless reasonable grounds exist for the executive committee to withhold such ratification.

a. Each temporary committee shall be entitled, unless inconsistent with the provisions of this constitution, to make rules and regulations relating to the conduct of its own activities including, if necessary, the appointment of a chairperson.

a. Such temporary committee may include -

i. a nomination committee consisting of at least three members (at least one of whom shall not be a member of the executive committee) and which shall be constituted as soon as reasonably possible prior to the annual general meeting and shall be tasked with procuring nominations in respect of the officers and the chairperson of each of the standing committees to be elected at the annual general meeting;

i. an audit committee to assist the treasurer generally and specifically to ensure the accuracy of the accounting records and to verify the accuracy of the financial report prepared by the treasurer for submission to the annual general meeting and to ISOC;

i. regional committees.

1. **PROCEEDINGS OF COMMITTEES**

a. The members of each of the executive committee, the standing committees and the temporary committees, if any, may -

i. meet, adjourn and otherwise regulate their meetings as they think fit and any member of the committee shall be entitled to convene a meeting of such committee;

ii. determine what notice shall be given of their meetings and the means of giving that notice, provided that any such prior determination may be varied, depending on the circumstances and reasons for the committee meeting in question.

a. Unless otherwise determined by ISOC-ZA in general meeting, or by a meeting of the members of such committee at which all the members of such committee are present, the quorum necessary for the transaction of the business of such committee shall be a majority of the members of such committee for the time being in

Stellenbosch University http://scholar.sun.ac.za

office. A resolution of members of such committee shall be passed by a majority of the votes of the members of such committee present at the meeting at which it is proposed.

a. A resolution which has been signed by the majority of members of a committee and inserted in the minute book of such committee, shall be as valid and effective as if it had been passed at a meeting of such committee. Any such resolution may consist of several documents, each of which may be signed by one or more members of the committee and such resolution shall be deemed to have been passed on the date on which it was signed by the last member of the committee who signed it (unless a statement to the contrary is made in that resolution). Signature of a resolution may include signature by electronic means (specifically including signature by electronic mail) subject to such verification procedures as the members of the committee in question may deem appropriate in the circumstances.

1. **GENERAL MEETINGS**

a. All members shall be entitled to attend and speak at general meetings of ISOC-ZA and general meetings shall not be held at any venue which is not open and accessible to all members of the society. Provided that the provisions of this clause 15.1 shall not be contravened by the holding of a general meeting in any one geographical location in the RSA; provided further that ISOC-ZA shall use all reasonable endeavours to assist members who are situate or resident in any geographical location in the RSA other than that at which the general meeting will be held, to attend or participate in such general meeting, by way of electronic or other means including, in particular, video conferencing.

a. An annual general meeting shall be held once in each year, if possible prior to the end of the financial year on 30 June, at such time and place as may be determined by the executive committee.

a. Further general meetings may be held from time to time and as the executive committee deems necessary, at such times and places as may be determined by the executive committee.

a. Notice of every general meeting, including the annual general meeting, shall be given to all members in terms of clause 28 and shall state the place, day and hour of, and the nature of the business to be transacted at the general meeting. The chairperson shall cause such notice to be given to each member not less than seven days in advance of that general meeting.

a. The general meeting shall be the highest managing authority of ISOC-ZA and shall be responsible for the control and monitoring of the business of ISOC-ZA.

a. All members shall be entitled to appoint a proxy to attend, speak and vote (whether on a show of hands or on a poll) in their stead at any general meeting in accordance with this constitution.

1. **PROCEEDINGS AT GENERAL MEETINGS**

a. Unless a general meeting determines that there shall be another quorum, a quorum for a general meetings shall be 10% of the members of ISOC-ZA or twenty-five members, whichever is the greater, which members shall be present in person, represented by an authorised representative or proxy or participating by video conference or such other electronic means which will allow participation in the discussion and/or voting which may take place at such general meeting, without any unreasonable delay. The executive committee shall be entitled, in its sole discretion, to determine the reasonableness of any delay relating to the participation of any member or members by electronic means.

a. Should a quorum not be present within thirty minutes after the appointed time for a general meeting, the general meeting shall be dissolved and shall stand adjourned to the same day (or if that day is a public holiday, the next business day) in the next week at the same time and place, and a quorum at the resumption of the

Stellenbosch University http://scholar.sun.ac.za

general meeting shall be the members present in person or by proxy at that meeting.

a. No official business of ISOC-ZA shall be conducted at a general meeting unless a quorum is present.

a. The chairperson or, failing him or her, the vice-chairperson shall be the chair of each general meeting, provided that if the chairperson and vice-chairperson is not present and/or willing to act, the members present shall elect one of the members of the executive committee or, if no member of the executive committee is present and/or willing to act, elect a member to be the chair of that general meeting.

a. The chair of a general meeting may, in his or her discretion or in any other circumstance, adjourn that general meeting from time to time.

a. It shall not be necessary to give notice of any adjournment of a general meeting.

a. No business shall be transacted at the resumption of any adjourned general meeting other than the business left unfinished at the general meeting from which the adjournment took place.

b. The general meeting is empowered to deal with, inter alia, the following -

i. the making of broad policy directives to be implemented by the executive committee;

i. the acceptance of the report of the secretary, committee, the annual financial report and the appointment of auditors on the recommendation of the executive committee;

i. consideration of any recommendations made by the executive committee;

i. the amendment of this constitution in terms of clause 31;

i. the discussion of motions concerning the interests and rights of members placed on the agenda by members, the executive committee or the chairperson in consultation with the executive committee, at least ten business days before the general meeting;

i. the fees payable by members from time to time;

i. any other matter that can properly be raised at a general meeting of ISOC-ZA.

a. At any general meeting, including the annual general meeting at which the election of the officers and the chairperson of each of the standing committees takes place in terms of clause 18, each member who is present in person, by authorised representative or by proxy shall have one vote on a show of hands or on a poll. In addition, electronic voting by members participating in such general meeting (by means of video conferencing or otherwise) shall be permitted both on a show of hands and on a poll.

a. At any general meeting a resolution put to the vote shall be decided by a show of hands unless a poll is demanded.

a. On a show of hands at a general meeting a declaration in good faith by the chair of such meeting as to the result of the voting on any particular resolution and an entry to that effect in the minutes shall be conclusive proof of that result, without proof of the number or proportions of votes recorded in favour of, against and as abstaining from such resolution.

a. If a poll is demanded at a general meeting -

i. on a resolution regarding the election of the chair of such general meeting, the poll shall be taken immediately and in such manner as the general meeting determines, and a poll on any other resolution shall be taken at such time and in such manner as the chair of the general meeting directs;

Stellenbosch University http://scholar.sun.ac.za

i. the result of the poll shall be deemed to be a resolution of the general meeting at which the poll was demanded;

i. the demand shall not preclude the general meeting from considering any question other than that on which the poll has been demanded unless the general meeting decides otherwise;

i. the demand may be withdrawn at any time.

a. No objection shall be taken to the admission or rejection of any vote except at the general meeting at which the vote in dispute is cast, or, if it is adjourned, the resumption thereof. The chair of that general meeting or resumed general meeting shall determine any issue raised by such objection and his or her determination shall be final and binding.

a. A resolution in writing signed by a majority of members, or a special resolution signed by [ ]% of the members, entitled to receive notice of and to attend and vote at a general meeting shall be as valid and effective as if it had been passed at a general meeting properly called and held. Any such resolution may consist of several documents, each of which may be signed by one or more members and shall be deemed to have been passed on the date on which it was signed by the last member who signed it, unless a statement to the contrary is made in that resolution. Signature of a resolution may be made by electronic means, specifically including electronic mail, subject to such verification procedures as the executive committee, in their sole discretion may consider necessary.

1. **PROXIES**

a. A proxy form, power of attorney or other authority in respect of a general meeting shall be in writing and signed by or on behalf of the grantor.

a. A proxy form shall -

i. be in such form as is approved or accepted by the executive committee, it being specifically recorded that the members shall be entitled to vote on any ballot by electronic mail. Unless such electronic mail message indicates otherwise, such electronic mail message shall constitute the chair of the general meeting as such member's proxy to vote on any resolution or in the election of any officer or the chairperson of any standing committee in accordance with the instruction of the member contained in such electronic mail message;

i. be deposited at the registered address of ISOC-ZA or transmitted by electronic means to the electronic mail address of ISOC-ZA, to be received by ISOC-ZA not less than twenty-four hours before the time appointed for the holding of the general meeting, or resumption of an adjourned general meeting at which the person named therein proposes to vote; provided that the executive committee shall use all reasonable endeavours to provide electronic facilities for participation in and voting at general meetings simultaneously with the occurrence of such general meeting;

i. except insofar as it provides otherwise, be deemed to confer the power generally to act at the general meeting in question, subject to any specific direction as to the manner of voting;

i. be valid at every resumption of an adjourned meeting to which it relates, unless the contrary is stated thereon;

i. not be used at the resumption of an adjourned general meeting if it could not have been used at the general meeting from which it was adjourned for any reason other than that it was not lodged timeously for the meeting from which the adjournment took place;

i. not be valid after the expiry of two months after the date when it was signed and/or transmitted, whichever is the later, unless it specifically provides otherwise.

Stellenbosch University http://scholar.sun.ac.za

a. A vote cast or act done in accordance with the terms of a proxy form shall be deemed to be valid notwithstanding -

i. the previous death, insanity, or any other legal disability of the person appointing the proxy; or

i. the revocation of the proxy,

unless notice as to any of the abovementioned matters shall have been received by ISOC-ZA at its registered address or by the chair of the meeting at the place of the general meeting if not held at the registered address, before the commencement or resumption (if adjourned) of the general meeting at which the vote was cast or the act was done or before the poll on which the vote was cast.

1. **PROCEDURE FOR ELECTION OF OFFICERS AND THE CHAIRPERSON OF EACH STANDING COMMITTEE**

a. The elections of the officers and the chairperson of each standing committee shall be held at the general meeting convened in terms of clause 15 to adopt this constitution.

a. All elections of the officers and the chairperson of each standing committee subsequent to the elections referred to in clause 18.1 shall be held as follows -

i. such elections shall take place at the annual general meeting;

i. the chairperson shall, not less than twenty-one days before the annual general meeting, call for nominations of candidates for the positions of the officers and the chairperson of each of the standing committees and if a nomination committee has been constituted as a temporary committee, shall call upon such nomination committee to procure nominations as aforesaid, provided that the constitution of a nomination committee shall not preclude any member from nominating him or herself or any other member for election;

i. each nomination shall be in writing, shall be signed by the member nominating the nominee, shall include acceptance by the nominee of his or her nomination, shall indicate the position or positions in respect of which the nominee has been nominated and shall be submitted to the executive committee at least five days prior to the annual general meeting;

i. the executive committee shall advise all the members at the annual general meeting of the names of the nominees and the position or positions in respect of which they have been nominated;

i. the election of the officers and the chairperson of each of the standing committee shall take place by a show of hands unless a secret ballot has been requested. Any officer, member of the executive committee and/or chairperson of a standing committee shall cease to hold office upon the dissolution of ISOC-ZA in terms of clause 32 or if such person -

(1) dies, is declared insolvent or becomes of unsound mind or is found guilty of committing a serious criminal offence;

(1) resigns, by written notice to the chairperson;

(1) is absent for more than three consecutive general meetings or meetings of the executive committee, without the prior approval or subsequent ratification of the executive committee;

(1) is prohibited from being or is removed as or is disqualified from acting as a director of a company in terms of the Companies Act, 61 of 1973; or

(1) is given notice, signed by more than 50% of all of the members then entitled to vote at a general meeting, of the termination of his appointment.

Stellenbosch University http://scholar.sun.ac.za

a. The members of the executive committee may be paid any travelling, subsistence and other expenses properly incurred by them in the execution of their duty in or about the business of ISOC-ZA and which expenses are authorised or ratified by the executive committee.

1. **POWERS**

a. ISOC-ZA shall have all the powers necessary to enable it to achieve its objectives.

a. ISOC-ZA shall, without limitation of clause 19.1, have the following particular powers -

i. to negotiate on behalf of the members in respect of any broad policy directive laid down by the members;

i. to levy membership fees or other charges on its members;

i. to hire, purchase, possess or otherwise acquire movable or immovable property, to erect and maintain buildings thereon and to let, pledge, encumber or dispose of such property for the benefit and purposes of ISOC-ZA;

i. to enter into agreements with the state, any person or entity for the performance of any specific act or function or the rendering of a specific service;

i. to insure itself against any loss, damage, risk or liability which it may suffer or incur;

i. to lend, invest, put out on interest, deposit, advance or otherwise deal with such money which is not immediately required to cover the current expenditure of ISOC-ZA upon such security and in such manner as the executive committee may from time to time determine, and to realise such investment, vary, re-invest or otherwise deal therewith as the executive committee may from time to time determine; provided that any funds available for investment may only be invested with a registered financial institution as defined in section 1 of the Financial Institutions (Investments of Funds) Act 39 of 1984, as amended (or any statutory substitution of this Act) or in securities listed on any licenced stock exchange as defined in the Stock Exchanges Control Act 1 of 1985, as amended (or any statutory substitution of this Act);

i. to appoint employees to assist in the performance of its functions and to dismiss any of them;

i. to provide for remuneration, retirement, disability or other benefits for employees of ISOC-ZA;

i. to open, operate or close bank accounts in the name of ISOC-ZA;

i. to do all such other things as are incidental or conducive to the interests of ISOC-ZA and its members or to the attainment of all or any of the above objectives.

a. Notwithstanding anything to the contrary contained in this constitution, ISOC-ZA shall neither carry on any profit making activities nor participate in any business, profession or occupation, carried on by any of its members, nor provide any financial assistance to its members for the purpose of carrying on any business, profession or occupation by them.

1. **CERTIFICATES**

Certificates of membership may be issued under the authority of the executive committee in such manner and form as the executive committee may determine from time to time.

Stellenbosch University http://scholar.sun.ac.za

1. **DISTRIBUTION OF INCOME**

a. No part of the income or property of ISOC-ZA shall be distributed to its members, and the same shall be applied solely towards the pursuit of ISOC-ZA's purposes and objects, provided that this article shall not be construed as prohibiting the payment of expenses to members of the executive committee as provided for in clause 18.3 or the payment of remuneration to employees.

a. Disbursements by ISOC-ZA shall be made by the treasurer on its behalf provided that the prior approval of the executive committee shall be required in respect of disbursements in excess of such amount as may be determined by the executive committee from time to time and such approval shall be recorded in the minutes of the executive committee meeting at which it was given.

1. **WINDING UP**

If ISOC-ZA is wound up (whether voluntarily or compulsorily) or dissolved, the assets remaining after payment of the liabilities of ISOC-ZA and the costs of winding up shall be given or transferred to one or more associations, companies or institutions having objects similar to the main object of ISOC-ZA, to be determined by the members of ISOC-ZA at or before the time of its winding up or dissolution in consultation with the Vice-President of Chapters of ISOC, or failing such determination by such court as may have jurisdiction in respect thereof.

1. **FEES**

a. Subject to the provisions of clause 23.3, members shall pay to ISOC-ZA the membership fees as determined by the executive committee and ratified by the members in general meeting, from time to time.

a. Each member shall pay such membership fees to ISOC-ZA at such time or times and on such terms as the executive committee may determine.

a. The executive committee shall be entitled to determine, subject to the ratification of the members in general meeting, different fees for the different classes of membership of ISOC-ZA and shall further be entitled to subsidise, reduce or waive the membership fees of any member in the event of financial hardship.

1. **FINANCIAL YEAR**

The financial year of ISOC-ZA shall run from 1 July to 30 June of each year.

1. **AUDITORS**

The ISOC-ZA shall not appoint auditors unless required to do so by law, in which event -

a. the auditors shall be appointed by ISOC-ZA in general meeting; and

a. the remuneration of the auditors shall be determined by such general meeting.

1. **INTERPRETATION OF CONSTITUTION**

In the event of any dispute arising out of any provisions of this constitution, such dispute shall be referred in writing for determination in accordance with the provisions of clause 33, which shall apply, mutatis mutandis, in respect of any dispute arising as to the interpretation or intention of any provisions of this constitution.

1. **INDEMNITY**

Every member of the executive committee and any person employed by ISOC-ZA shall be indemnified out of ISOC-ZA's funds against all liability incurred by him in defending any proceedings (whether civil or criminal) arising out of any actual or alleged negligence, default, breach of duty or breach of trust on his part in relation to ISOC-ZA in which judgment is given in his favour or in which he is acquitted or in connection with any matter in which relief is granted to him by the Court.

Stellenbosch University http://scholar.sun.ac.za

1. **NOTICES**

a. Subject to the provisions of this constitution, a notice shall be in writing and shall be given or served by ISOC-ZA upon its members or the members of the executive committee either by delivery or by sending it properly addressed, to -

i. a member at the address, telefacsimile number or electronic mail address (if any), shown in the register of members;

i. a member of the executive committee at the address, telefacsimile number or electronic mail address (if any), shown in the register of members of the executive committee.

a. A member may by notice require ISOC-ZA to record a physical address or telefacsimile address within the RSA or an electronic mail address, which shall be deemed to be his address for the purpose of the service of notices.

a. Every such notice shall be deemed, until the contrary is proved, to have been received -

i. if it is delivered, on the date on which it is so delivered;

i. if it is sent by post, ten days after the date on which it posted;

i. if it is sent by electronic mail or telefacsimile, on the date of successful transmission.

a. When a given number of days' notice or notice over any period is required to be given, the date on which it is deemed to be received shall not be counted in such number of days or period.

a. The provisions of this clause 28 shall not invalidate any notice given other than as provided for in this clause 28.

a. The omission to give notice of a general meeting or a meeting of the executive committee, or the non-receipt of, or delay in transmission through the post of any such notice by or to any member or member of the executive committee, as the case may be, shall not invalidate any resolution passed at any such meeting.

1. **RULES**

The members may, by ordinary resolution, adopt and amend such rules as they may deem appropriate for the purposes of regulating the conduct of the members. All members agree to be bound by the provisions of such rules. Such rules may include provisions for the payment of fines to ISOC-ZA by members if they breach such rules, the amount of such fines to be stipulated in such rules. The payment of or liability to pay a fine by a member as a result of a breach of such rules by that member shall not preclude the termination of that member's membership in terms of clause 7.10 as a result of such breach.

1. **BANK ACCOUNT**

The members of the executive committee shall be entitled to open and operate a bank account on the basis that such bank account shall only be operated upon the signature of two members of the executive committee, one of whom shall be the treasurer.

1. **AMENDMENT OF CONSTITUTION**

This constitution shall only be amended by the members in general meeting; provided that -

a. notice in writing of such amendment shall have been given to the executive committee not less than thirty-five days before the general meeting at which the amendment is to be considered. The executive committee shall notify each member in writing of any such proposed amendment not less than twenty-one days before that general meeting;

a. the quorum at a general meeting constituted to consider any such proposed amendment shall be the majority in

Stellenbosch University http://scholar.sun.ac.za

number of the members of ISOC-ZA, present in person, participating through an electronic facility or represented by an authorised representative or proxy;

a. the amendment, subject to such modifications as may be required at such general meeting, is approved of by a special resolution;

a. the amendment, as approved in terms of clause 31.3 above, is approved by the Commissioner for Inland Revenue; and

a. the amendment is approved prior to its adoption, or ratified subsequently thereto, by the Vice-President of Chapters of ISOC.

1. **DISSOLUTION OF ISOC-ZA**

a. ISOC-ZA may be dissolved by the passing of a special resolution to that effect by a general meeting convened for the sole purpose of considering such dissolution.

a. At least twenty-one days notice shall be given of the aforesaid meeting and the notice shall clearly state that the question of dissolution of ISOC-ZA and the disposal of its assets will be considered.

a. A quorum at such meeting shall be the majority in number of the members of ISOC, present in person, by means of an electronic facility or represented by an authorised representative or proxy.

a. If no quorum is present at such general meeting, that meeting shall stand adjourned by not less than one week and the members attending the adjourned meeting shall constitute a quorum of such adjourned meeting.

1. **DISPUTES**

a. If any dispute of whatever nature pursuant to this constitution, the activities of ISOC-ZA or the dissolution of ISOC-ZA arises, any member shall be entitled to require, by written notice to the others of them, that the dispute be referred for determination to an expert pursuant to this clause 33.

a. The expert shall be, if the question in issue is -

i. primarily an accounting matter, an independent practising accountant of not less than fifteen years standing;

i. primarily a legal matter, a practising Senior Counsel or attorney of not less than fifteen years standing;

i. any other matter, an independent person,

agreed upon by the members or, failing such agreement within three days after the date on which the determination is called for in terms of clause 33.1, appointed by the Chairman of the Johannesburg Bar Council who may be instructed by any member to make that nomination at any time after the expiry of that three day period.

a. The expert selected as aforesaid shall in all respects act as an expert and not as an arbitrator.

a. The expert shall not be bound to follow principles of law but may decide the matter/s submitted to him according to what he considers just and equitable in the circumstances.

a. Any hearing by the expert shall be held at such place as may be agreed upon by the parties thereto, and failing such agreement, in Johannesburg.

a. Immediately after the expert has been appointed, he may be called upon by any member to fix a date and place when and where the proceedings shall be held and to settle the procedure and manner in which the proceedings will be held.

Stellenbosch University http://scholar.sun.ac.za

a. The members shall use their best endeavours to procure that the decision of the expert shall be given within twenty-one days or so soon thereafter as possible after it has been called for.

a. The expert's decision shall be final and binding on all members affected thereby, shall be carried into effect and may be made an order of any competent court at the instance of any of the members.

a. Upon giving his award, the expert shall deliver to the parties to the dispute a written statement setting out -

i. the findings of fact determined by him and forming the basis of his award; and

i. full reasons justifying his award.

a. This clause constitutes an irrevocable consent by the members to any proceedings in terms hereof and no member shall be entitled to withdraw therefrom or to claim at any such proceedings that it is not bound by this clause 33.

a. This clause is severable from the rest of this agreement and shall remain in effect even if this constitution is varied for any reason or ISOC-ZA is dissolved in accordance with this constitution.

Stellenbosch University http://scholar.sun.ac.za

BYLAE F:
GOVERNMENT GAZETTE: ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

Stellenbosch University http://scholar.sun.ac.za

Government Gazette

REPUBLIC OF SOUTH AFRICA

Vol. 446 Cape Town 2 August 2002 No. 23708

THE PRESIDENCY

No. 1046 2 August 2002

It is hereby notified that the President has assented to the following Act, which is hereby published for general information:–

No. 25 of 2002: Electronic Communications and Transactions Act, 2002.

AIDS HELPLINE: 0800-123-22 Prevention is the cure

(English text signed by the President.)
(Assented to 31 July 2002.)

ACT

To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:—

ARRANGEMENT OF SECTIONS

Sections

Stellenbosch University http://scholar.sun.ac.za

Stellenbosch University http://scholar.sun.ac.za

CHAPTER I

INTERPRETATION, OBJECTS AND APPLICATION

Definitions

1. In this Act, unless the context indicates otherwise—

"addressee", in respect of a data message, means a person who is intended by the originator to receive the data message, but not a person acting as an intermediary in respect of that data message;

"advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37;

"authentication products or services" means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider" means a person whose authentication products or services have been accredited by the Accreditation Authority under section 37 or recognised under section 40;

"Authority" means the .za Domain Name Authority;

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment;

"browser" means a computer program which allows a person to read hyperlinked data messages;

"cache" means high speed memory that stores data for relatively short periods of time, under computer control, in order to speed up data transmission or processing;

"ccTLD" means country code domain at the top level of the Internet's domain name system assigned according to the two-letter codes in the International Standard ISO 3166-1 (Codes for Representation of Names of Countries and their Subdivision);

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message;

"consumer" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

"Consumer Affairs Committee" means the Consumer Affairs Committee established by section 2 of the Consumer Affairs (Unfair Business Practices) Act, 1988 (Act No. 71 of 1988);

"critical data" means data that is declared by the Minister in terms of section 53 to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens;

"critical database" means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted;

"critical database administrator" means the person responsible for the management and control of a critical database;

Stellenbosch University http://scholar.sun.ac.za

"cryptography product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—

(a) that such data can be accessed only by relevant persons;

(b) the authenticity of the data;

(c) the integrity of the data; or

(d) that the source of the data can be correctly ascertained;

"cryptography provider" means any person who provides or who proposes to provide cryptography services or products in the Republic;

"cryptography service" means any service which is provided to a sender or a recipient of a data message or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—

(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;

(b) that the authenticity or integrity of such data or data message is capable of being ascertained;

(c) the integrity of the data or data message; or

(d) that the source of the data or data message can be correctly ascertained;

"cyber inspector" means an inspector referred to in Chapter XII;

"data" means electronic representations of information in any form;

"data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

"data message" means data generated, sent, received or stored by electronic means and includes—

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;

"data subject" means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

"Department" means the Department of Communications;

"Director-General" means the Director-General of the Department;

"domain name" means an alphanumeric designation that is registered or assigned in respect of an electronic address or other resource on the Internet;

"domain name system" means a system to translate domain names into IP addresses or other information;

"e-government services" means any public service provided by electronic means by any public body in the Republic;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

"electronic communication" means a communication by means of data messages;

"electronic signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;

"e-mail" means electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication;

"home page" means the primary entry point web page of a web site;

"hyperlink" means a reference or link from some point in one data message directing a browser or other technology or functionality to another data message or point therein or to another place in the same data message;

"ICANN" means the Internet Corporation for Assigned Names and Numbers, a California non-profit public benefit corporation established in terms of the laws of the state of California in the United States of America;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet;

"information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

"Internet" means the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof;

"IP address" means the number identifying the point of connection of a computer or other device to the Internet;

"Minister" means the Minister of Communications;

"originator" means a person by whom, or on whose behalf, a data message purports to have been sent or generated prior to storage, if any, but does not include a person acting as an intermediary with respect to that data message;

"person" includes a public body;

"personal information" means information about an identifiable individual, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol, or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but excludes information about an individual who has been dead for more than 20 years;

"prescribe" means prescribe by regulation under this Act;

"private body" means—

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person,

but not a public body;

"public body" means—

(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

(b) any other functionary or institution when—

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a power or performing a function in terms of any legislation;

"registrant" means an applicant for or holder of a domain name;

"registrar" means an entity which is licensed by the Authority to update a repository;

Stellenbosch University http://scholar.sun.ac.za

"registry" means an entity licensed by the Authority to manage and administer a specific subdomain;

"repository" means the primary register of the information maintained by a registry;

"second level domain" means the subdomain immediately following the ccTLD;

"SMMEs" means Small, Medium and Micro Enterprises contemplated in the Schedules to the Small Business Development Act, 1996 (Act No. 102 of 1996);

"subdomain" means any subdivision of the .za domain name space which begins at the second level domain;

"TCP/IP" means the Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet;

"TLD" means a top level domain of the domain name system;

"third party", in relation to a service provider, means a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems;

"transaction" means a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services;

"universal access" means access by all citizens of the Republic to Internet connectivity and electronic transactions;

"WAP" means Wireless Application Protocol, an open international standard developed by the Wireless Application Protocol Forum Limited, a company incorporated in terms of the laws of the United Kingdom, for applications that use wireless communication and includes Internet access from a mobile phone;

"web page" means a data message on the World Wide Web;

"web site" means any location on the Internet containing a home page or web page;

"World Wide Web" means an information browsing framework that allows a user to locate and access information stored on a remote computer and to follow references from one computer to related information on another computer; and

".za domain name space" means the .za ccTLD assigned to the Republic according to the two-letter codes in the International Standard ISO 3166-1.

Objects of Act

2. (1) The objects of this Act are to enable and facilitate electronic communications and transactions in the public interest, and for that purpose to—

(a) recognise the importance of the information economy for the economic and social prosperity of the Republic;

(b) promote universal access primarily in underserviced areas;

(c) promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic;

(d) remove and prevent barriers to electronic communications and transactions in the Republic;

(e) promote legal certainty and confidence in respect of electronic communications and transactions;

(f) promote technology neutrality in the application of legislation to electronic communications and transactions;

(g) promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;

(h) ensure that electronic transactions in the Republic conform to the highest international standards;

(i) encourage investment and innovation in respect of electronic transactions in the Republic;

(j) develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;

(k) promote the development of electronic transactions services which are responsive to the needs of users and consumers;

(l) ensure that, in relation to the provision of electronic transactions services, the special needs of particular communities and, areas and the disabled are duly taken into account;

(m) ensure compliance with accepted International technical standards in the provision and development of electronic communications and transactions;

(n) promote the stability of electronic transactions in the Republic;

(o) promote the development of human resources in the electronic transactions environment;

(p) promote SMMEs within the electronic transactions environment;

(q) ensure efficient use and management of the .za domain name space; and

(r) ensure that the national interest of the Republic is not compromised through the use of electronic communications.

Interpretation

3. This Act must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act.

Sphere of application

4. (1) Subject to any contrary provision in this section, this Act applies in respect of any electronic transaction or data message.

(2) This Act must not be construed as—

(a) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form; or

(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

(3) The sections of this Act mentioned in Column B of Schedule 1 do not apply to the laws mentioned in Column A of that Schedule.

(4) This Act must not be construed as giving validity to any transaction mentioned in Schedule 2.

(5) This Act does not limit the operation of any law that expressly authorises, prohibits or regulates the use of data messages, including any requirement by or under a law for information to be posted or displayed in a specified manner, or for any information or document to be transmitted by a specified method.

CHAPTER II

MAXIMISING BENEFITS AND POLICY FRAMEWORK

Part 1

National e-strategy

National e-strategy

5. (1) The Minister must, within 24 months after the promulgation of this Act, develop a three-year national e-strategy for the Republic, which must be submitted to the Cabinet for approval.

(2) The Cabinet must, on acceptance of the national e-strategy, declare the implementation of the national e-strategy as a national priority.

(3) The Minister, in developing the national e-strategy as envisaged in subsection (1)—

(a) must determine all matters involving e-government services in consultation with the Minister for the Public Service and Administration;

(b) must determine the roles of each person, entity or sector in the implementation of the national e-strategy;

(c) must act as the responsible Minister for co-ordinating and monitoring the implementation of the national e-strategy;

(d) may make such investigations as he or she may consider necessary;

Stellenbosch University http://scholar.sun.ac.za

(e) may conduct research into and keep abreast of developments relevant to electronic communications and transactions in the Republic and internationally;

(f) must continually survey and evaluate the extent to which the objectives of the national e-strategy have been achieved;

(g) may liaise, consult and cooperate with public bodies, the private sector or any other person; and

(h) may, in consultation with the Minister of Finance, appoint experts and other consultants on such conditions as the Minister may determine.

(4) *(a)* The Minister must, in consultation with other members of the Cabinet, determine the subject matters to be addressed in the national e-strategy and the principles that must govern the implementation thereof.

(b) Prior to prescribing any subject matter and principles provided for in paragraph *(a)*, the Minister must invite comments from all interested parties by notice in the *Gazette* and consider any comments received.

(c) The national e-strategy must, amongst others, set out—

(i) the electronic transactions strategy of the Republic, distinguishing between regional, national, continental and international strategies;

(ii) programmes and means to achieve universal access, human resource development and development of SMMEs as provided for in this Part;

(iii) programmes and means to promote the overall readiness of the Republic in respect of electronic transactions;

(iv) ways to promote the Republic as a preferred provider and user of electronic transactions in the international market;

(v) existing government initiatives directly or indirectly relevant to or impacting on the national e-strategy and, if applicable, how such initiatives are to be utilised in attaining the objectives of the national e-strategy;

(vi) the role expected to be performed by the private sector in the implementation of the national e-strategy and how government can solicit the participation of the private sector to perform such role;

(vii) the defined objectives, including time frames within which the objectives are to be achieved; and

(viii) the resources required to achieve the objectives provided for in the national e-strategy.

(5) Upon approval by the Cabinet, the Minister must publish the national e-strategy in the *Gazette*.

(6) For purposes of achieving the objectives of the national e-strategy, the Minister may, in consultation with the Minister of Finance—

(a) procure funding from sources other than the State;

(b) allocate funds for implementation of the national e-strategy to such institutions and persons as are responsible for delivery in terms of the national e-strategy and supervise the execution of their mandate; and

(c) take any steps necessary to enable all relevant parties to carry out their respective obligations.

(7) The Minister must annually report to the Cabinet on progress made and objectives achieved or outstanding and may include any other matter the Minister deems relevant.

(8) The Minister must annually review the national e-strategy and where necessary make amendments thereto in consultation with all relevant members of the Cabinet.

(9) No amendment or adaptation of the national e-strategy is effective unless approved by the Cabinet.

(10) The Minister must publish any material revision of the national e-strategy in the *Gazette*.

(11) The Minister must table an annual report in Parliament regarding the progress made in the implementation of the national e-strategy.

Universal access

6. In respect of universal access, the national e-strategy must outline strategies and programmes to—

(a) provide Internet connectivity to disadvantaged communities;

(b) encourage the private sector to initiate schemes to provide universal access;

(c) foster the adoption and use of new technologies for attaining universal access; and

(d) stimulate public awareness, understanding and acceptance of the benefits of Internet connectivity and electronic transacting.

Previously disadvantaged persons and communities

7. The Minister, in developing the national e-strategy, must provide for ways of maximising the benefits of electronic transactions to historically disadvantaged persons and communities, including, but not limited to—

(a) making facilities and infrastructure available or accessible to such persons and communities to enable the marketing and sale of their goods or services by way of electronic transactions;

(b) providing or securing support services for such facilities and infrastructure to assist with the efficient execution of electronic transactions; and

(c) rendering assistance and advice to such persons and communities on ways to adopt and utilise electronic transactions efficiently.

Development of human resources

8. (1) The Minister, in developing the national e-strategy, must provide for ways of promoting development of human resources set out in this section within the context of the government's integrated human resource development strategies, having regard to structures and programmes that have been established under existing laws.

(2) The Minister must consult with the Ministers of Labour and Education on existing facilities, programmes and structures for education, training and human resource development in the information technology sector relevant to the objects of this Act.

(3) Subject to subsections (1) and (2), the Minister must promote skills development in the areas of—

(a) information technology products and services in support of electronic transactions;

(b) business strategies for SMMEs and other businesses to utilise electronic transactions;

(c) sectoral, regional, national, continental and international policy formulation for electronic transactions;

(d) project management on public and private sector implementation of electronic transactions;

(e) the management of the .za domain name space;

(f) the management of the IP address system for the African continent in consultation with other African states;

(g) convergence between communication technologies affecting electronic transactions;

(h) technology and business standards for electronic transactions;

(i) education on the nature, scope, impact, operation, use and benefits of electronic transactions; and

(j) any other matter relevant to electronic transactions.

SMMEs

9. The Minister must, in consultation with the Minister of Trade and Industry, evaluate the adequacy of any existing processes, programmes and infrastructure providing for the utilisation by SMMEs of electronic transactions and, pursuant to such evaluation, may—

(a) establish or facilitate the establishment of electronic communication centres for SMMEs;

Stellenbosch University http://scholar.sun.ac.za

(b) facilitate the development of web sites or web site portals that will enable SMMEs to transact electronically and obtain information about markets, products and technical assistance; and

(c) facilitate the provision of such professional and expert assistance and advice to SMMEs on ways to utilise electronic transacting efficiently for their development.

Part 2

Electronic transactions policy

Electronic transactions policy

10. (1) The Minister must, subject to this Act, formulate electronic transactions policy.

(2) In formulating the policy contemplated in subsection (1), the Minister must—

(a) act in consultation with members of the Cabinet directly affected by such policy formulation or the consequences thereof;

(b) have due regard to—

(i) the objects of this Act;

(ii) the nature, scope and impact of electronic transactions;

(iii) international best practice and conformity with the law and guidelines of other jurisdictions and international bodies; and

(iv) existing laws and their administration in the Republic.

(3) The Minister must publish policy guidelines in the *Gazette* on issues relevant to electronic transactions in the Republic.

(4) In implementing this Chapter, the Minister must encourage the development of innovative information systems and the growth of related industry.

CHAPTER III

FACILITATING ELECTRONIC TRANSACTIONS

Part 1

Legal requirements for data messages

Legal recognition of data messages

11. (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.

(2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.

(3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is—

(a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and

(b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

Writing

12. A requirement in law that a document or information must be in writing is met if the document or information is—

(a) in the form of a data message; and

(b) accessible in a manner usable for subsequent reference.

Signature

13. (1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if—

(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and

(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.

(4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that—

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred.

Original

14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if—

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1*(a)*, the integrity must be assessed—

(a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

Admissibility and evidential weight of data messages

15. (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence—

(a) on the mere grounds that it is constituted by a data message; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message must be given due evidential weight.

(3) In assessing the evidential weight of a data message, regard must be had to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the data message was maintained;

(c) the manner in which its originator was identified; and

(d) any other relevant factor.

Stellenbosch University http://scholar.sun.ac.za

(4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Retention

16. (1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if—

(a) the information contained in the data message is accessible so as to be usable for subsequent reference;

(b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Production of document or information

17. (1) Subject to section 28, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if—

(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for—

(a) the addition of any endorsement; or

(b) any immaterial change, which arises in the normal course of communication, storage or display.

Notarisation, acknowledgement and certification

18. (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

Other requirements

19. (1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms "document", "record", "file", "submit", "lodge", "deliver", "issue", "publish", "write in", "print" or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender.

Automated transactions

20. In an automated transaction—

(a) an agreement may be formed where an electronic agent performs an action required by law for agreement formation;

(b) an agreement may be formed where all parties to a transaction or either one of them uses an electronic agent;

(c) a party using an electronic agent to form an agreement is, subject to paragraph *(d)*, presumed to be bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement;

(d) A party interacting with an electronic agent to form an agreement is not bound by the terms of the agreement unless those terms were capable of being reviewed by a natural person representing that party prior to agreement formation.

(e) no agreement is formed where a natural person interacts directly with the electronic agent of another person and has made a material error during the creation of a data message and—

(i) the electronic agent did not provide that person with an opportunity to prevent or correct the error;

(ii) that person notifies the other person of the error as soon as practicable after that person has learned of it;

(iii) that person takes reasonable steps, including steps that conform to the other person's instructions to return any performance received, or, if instructed to do so, to destroy that performance; and

(iv) that person has not used or received any material benefit or value from any performance received from the other person.

Part 2

Communication of data messages

Variation by agreement between parties

21. This Part only applies if the parties involved in generating, sending, receiving, storing or otherwise processing data messages have not reached agreement on the issues provided for therein.

Stellenbosch University http://scholar.sun.ac.za

Formation and validity of agreements

22. (1) An agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages.

(2) An agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offeror.

Time and place of communications, dispatch and receipt

23. A data message—

(a) used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee:

(b) must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee: and

(c) must be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence.

Expression of intent or other statement

24. As between the originator and the addressee of a data message an expression of intent or other statement is not without legal force and effect merely on the grounds that—

(a) it is in the form of a data message; or

(b) it is not evidenced by an electronic signature but by other means from which such person's intent or other statement can be inferred.

Attribution of data messages to originator

25. A data message is that of the originator if it was sent by—

(a) the originator personally;

(b) a person who had authority to act on behalf of the originator in respect of that data message: or

(c) an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.

Acknowledgement of receipt of data message

26. (1) An acknowledgement of receipt of a data message is not necessary to give legal effect to that message.

(2) An acknowledgement of receipt may be given by—

(a) any communication by the addressee, whether automated or otherwise: or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

CHAPTER IV

E-GOVERNMENT SERVICES

Acceptance of electronic filing and issuing of documents

27. Any public body that, pursuant to any law—

(a) accepts the filing of documents, or requires that documents be created or retained:

(b) issues any permit, licence or approval; or

(c) provides for a manner of payment,

may, notwithstanding anything to the contrary in such law—

(i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages;

(ii) issue such permit, licence or approval in the form of a data message; or

(iii) make or receive payment in electronic form or by electronic means.

Requirements may be specified

28. (1) In any case where a public body performs any of the functions referred to in section 27, such body may specify by notice in the *Gazette*—

(a) the manner and format in which the data messages must be filed, created, retained or issued;

(b) in cases where the data message has to be signed, the type of electronic signature required;

(c) the manner and format in which such electronic signature must be attached to, incorporated in or otherwise associated with the data message;

(d) the identity of or criteria that must be met by any authentication service provider used by the person filing the data message or that such authentication service provider must be a preferred authentication service provider;

(e) the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of data messages or payments; and

(f) any other requirements for data messages or payments.

(2) For the purposes of subsection (1)*(d)* the South African Post Office Limited is a preferred authentication service provider and the Minister may designate any other authentication service provider as a preferred authentication service provider based on such authentication service provider's obligations in respect of the provision of universal access.

CHAPTER V

CRYPTOGRAPHY PROVIDERS

Register of cryptography providers

29. (1) The Director-General must establish and maintain a register of cryptography providers.

(2) The Director-General must record the following particulars in respect of a cryptography provider in that register:

(a) The name and address of the cryptography provider;

(b) a description of the type of cryptography service or cryptography product being provided; and

(c) such other particulars as may be prescribed to identify and locate the cryptography provider or its products or services adequately.

(3) A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.

Registration with Department

30. (1) No person may provide cryptography services or cryptography products in the Republic until the particulars referred to in section 29 in respect of that person have been recorded in the register contemplated in section 29.

(2) A cryptography provider must in the prescribed manner furnish the Director-General with the information required and pay the prescribed administrative fee.

(3) A cryptography service or cryptography product is regarded as being provided in the Republic if it is provided—

Stellenbosch University http://scholar.sun.ac.za

(*a*) from premises in the Republic;
(*b*) to a person who is present in the Republic when that person makes use of the service or product; or
(*c*) to a person who uses the service or product for the purposes of a business carried on in the Republic or from premises in the Republic.

Restrictions on disclosure of information

31. (1) Information contained in the register provided for in section 29 must not be disclosed to any person other than to employees of the Department who are responsible for the keeping of the register.

(2) Subsection (1) does not apply in respect of information which is disclosed—
(*a*) to a relevant authority which investigates a criminal offence or for the purposes of any criminal proceedings;
(*b*) to government agencies responsible for safety and security in the Republic, pursuant to an official request;
(*c*) to a cyber inspector;
(*d*) pursuant to section 11 or 30 of the Promotion of Access to Information Act, (Act No. 2 of 2000); or
(*e*) for the purposes of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

Application of Chapter and offences

32. (1) The provisions of this Chapter do not apply to the National Intelligence Agency established in terms of section 3 of the Intelligence Services Act, 1994 (Act No. 38 of 1994).

(2) A person who contravenes or fails to comply with a provision of this Chapter is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding two years.

CHAPTER VI

AUTHENTICATION SERVICE PROVIDERS

Part 1

Accreditation Authority

Definition

33. In this Chapter, unless the context indicates otherwise—
"accreditation" means recognition of an authentication product or service by the Accreditation Authority.

Appointment of Accreditation Authority and other officers

34. (1) For the purposes of this Chapter the Director-General must act as the Accreditation Authority.

(2) The Accreditation Authority, after consultation with the Minister, may appoint employees of the Department as Deputy Accreditation Authorities and officers.

Accreditation to be voluntary

35. Subject to section 30, a person may, without the prior authority of any other person, sell or provide authentication products or services in the Republic.

Powers and duties of Accreditation Authority

36. (1) The Accreditation Authority may—

(*a*) monitor the conduct, systems and operations of an authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act;
(*b*) temporarily suspend or revoke the accreditation of an authentication product or service; and
(*c*) appoint an independent auditing firm to conduct periodic audits of the authentication service provider to ensure its compliance with section 38 and the other obligations of authentication service providers in terms of this Act.

(2) The Accreditation Authority must maintain a publicly accessible database in respect of—
(*a*) authentication products or services accredited in terms of section 37;
(*b*) authentication products and services recognised in terms of section 40;
(*c*) revoked accreditations or recognitions; and
(*d*) such other information as may be prescribed.

Part 2

Accreditation

Accreditation of authentication products and services

37. (1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.

(2) An application for accreditation must—
(*a*) be made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and
(*b*) be accompanied by a non-refundable prescribed fee.

(3) A person falsely holding out its products or services to be accredited by the Accreditation Authority is guilty of an offence.

Criteria for accreditation

38. (1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—
(*a*) is uniquely linked to the user;
(*b*) is capable of identifying that user;
(*c*) is created using means that can be maintained under the sole control of that user; and
(*d*) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;
(*e*) is based on the face-to-face identification of the user.

(2) For purposes of subsection (1), the Accreditation Authority must have regard to the following factors in respect of an authentication service provider prior to accrediting authentication products or services:
(*a*) Its financial and human resources, including its assets;
(*b*) the quality of its hardware and software systems;
(*c*) its procedures for processing of products or services;
(*d*) the availability of information to third parties relying on the authentication product or service;
(*e*) the regularity and extent of audits by an independent body;
(*f*) the factors referred to in subsection (4) where the products and services are rendered by a certification service provider; and
(*g*) any other relevant factor which may be prescribed.

(3) For the purposes of subsections (2)(*b*) and (*c*), the hardware and software systems and procedures must at least—
(*a*) be reasonably secure from intrusion and misuse;
(*b*) provide a reasonable level of availability, reliability and correct operation;

Stellenbosch University http://scholar.sun.ac.za

(c) be reasonably suited to performing their intended functions; and
(d) adhere to generally accepted security procedures.

(4) For the purposes of subsection (1), where the products or services are provided by a certification service provider, the Accreditation Authority may stipulate, prior to accrediting authentication products or services—

(a) the technical and other requirements which certificates must meet;
(b) the requirements for issuing certificates;
(c) the requirements for certification practice statements;
(d) the responsibilities of the certification service provider;
(e) the liability of the certification service provider;
(f) the records to be kept and the manner in which and length of time for which they must be kept;
(g) requirements as to adequate certificate suspension and revocation procedures; and
(h) requirements as to adequate notification procedures relating to certificate suspension and revocation.

(5) The Accreditation Authority may impose any conditions or restrictions necessary when accrediting an authentication product or service.

Revocation or termination of accreditation

39. (1) The Accreditation Authority may suspend or revoke an accreditation if it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40.

(2) Subject to the provisions of subsection (3), the Accreditation Authority may not suspend or revoke the accreditation or recognition contemplated in subsection (1) unless it has—

(a) notified the authentication service provider in writing of its intention to do so;
(b) given a description of the alleged breach of any of the requirements, conditions or restrictions subject to which accreditation was granted under section 38 or recognition was given in terms of section 40; and
(c) afforded the authentication service provider the opportunity to—
  (i) respond to the allegations in writing; and
  (ii) remedy the alleged breach within a reasonable time.

(3) The Accreditation Authority may suspend accreditation granted under section 38 or recognition given under section 40 with immediate effect for a period not exceeding 90 days, pending implementation of the procedures required by subsection (2), if the continued accreditation or recognition of the authentication service provider is reasonably likely to result in irreparable harm to consumers or any person involved in an electronic transaction in the Republic.

(4) An authentication service provider whose products or services have been accredited in terms of this Chapter may terminate such accreditation at any time, subject to such conditions as may be agreed to at the time of accreditation or thereafter.

Accreditation of foreign products and services

40. (1) The Minister may, by notice in the *Gazette* and subject to such conditions as may be determined by him or her, recognise the accreditation or similar recognition granted to any authentication service provider or its authentication products or services in any foreign jurisdiction.

(2) An authentication service provider falsely holding out its products or services to have been recognised by the Minister in terms of subsection (1), is guilty of an offence.

Accreditation regulations

41. The Minister may make regulations in respect of—

(a) the rights and obligations of persons relating to the provision of accredited products and services;

(b) the manner in which the Accreditation Authority must administer and supervise compliance with those obligations;
(c) the procedure pertaining to the granting, suspension and revocation of accreditation;
(d) fees to be paid;
(e) information security requirements or guidelines; and
(f) any other relevant matter which it is necessary or expedient to prescribe for the proper implementation of this Chapter.

CHAPTER VII

CONSUMER PROTECTION

Scope of application

42. (1) This Chapter applies only to electronic transactions.

(2) Section 44 does not apply to an electronic transaction—

(a) for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;
(b) by way of an auction;
(c) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;
(d) for services which began with the consumer's consent before the end of the seven-day period referred to in section 44(1);
(e) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;
(f) where the goods—
  (i) are made to the consumer's specifications;
  (ii) are clearly personalised;
  (iii) by reason of their nature cannot be returned; or
  (iv) are likely to deteriorate or expire rapidly;
(g) where audio or video recordings or computer software were unsealed by the consumer;
(h) for the sale of newspapers, periodicals, magazines and books;
(i) for the provision of gaming and lottery services; or
(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is concluded, to provide these services on a specific date or within a specific period.

(3) This Chapter does not apply to a regulatory authority established in terms of a law if that law prescribes consumer protection provisions in respect of electronic transactions.

Information to be provided

43. (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction must make the following information available to consumers on the web site where such goods or services are offered:

(a) Its full name and legal status;
(b) its physical address and telephone number;
(c) its web site address and e-mail address;
(d) membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body;
(e) any code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;
(f) in the case of a legal person, its registration number, the names of its office bearers and its place of registration;
(g) the physical address where that supplier will receive legal service of documents;

Stellenbosch University http://scholar.sun.ac.za

(h) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;

(i) the full price of the goods or services, including transport costs, taxes and any other fees or costs;

(j) the manner of payment;

(k) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;

(l) the time within which the goods will be dispatched or delivered or within which the services will be rendered;

(m) the manner and period within which consumers can access and maintain a full record of the transaction;

(n) the return, exchange and refund policy of that supplier;

(o) any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer;

(p) the security procedures and privacy policy of that supplier in respect of payment, payment information and personal information;

(q) where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurrently; and

(r) the rights of consumers in terms of section 44, where applicable.

(2) The supplier must provide a consumer with an opportunity—

(a) to review the entire electronic transaction;

(b) to correct any mistakes; and

(c) to withdraw from the transaction, before finally placing any order.

(3) If a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.

(4) If a transaction is cancelled in terms of subsection (3)—

(a) the consumer must return the performance of the supplier or, where applicable, cease using the services performed; and

(b) the supplier must refund all payments made by the consumer minus the direct cost of returning the goods.

(5) The supplier must utilise a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned.

(6) The supplier is liable for any damage suffered by a consumer due to a failure by the supplier to comply with subsection (5).

Cooling-off period

44. (1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply—

(a) of goods within seven days after the date of the receipt of the goods; or

(b) of services within seven days after the date of the conclusion of the agreement.

(2) The only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment, which refund must be made within 30 days of the date of cancellation.

(4) This section must not be construed as prejudicing the rights of a consumer provided for in any other law.

Unsolicited goods, services or communications

45. (1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer—

(a) with the option to cancel his or her subscription to the mailing list of that person; and

(b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

Performance

46. (1) The supplier must execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise .

(2) Where a supplier has failed to execute the order within 30 days or within the agreed period, the consumer may cancel the agreement with seven days' written notice.

(3) If a supplier is unable to perform in terms of the agreement on the grounds that the goods or services ordered are unavailable, the supplier must immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification.

Applicability of foreign law

47. The protection provided to consumers in this Chapter, applies irrespective of the legal system applicable to the agreement in question.

Non-exclusion

48. Any provision in an agreement which excludes any rights provided for in this Chapter is null and void.

Complaints to Consumer Affairs Committee

49. A consumer may lodge a complaint with the Consumer Affairs Committee in respect of any non-compliance with the provisions of this Chapter by a supplier.

CHAPTER VIII

PROTECTION OF PERSONAL INFORMATION

Scope of protection of personal information

50. (1) This Chapter only applies to personal information that has been obtained through electronic transactions.

(2) A data controller may voluntarily subscribe to the principles outlined in section 51 by recording such fact in any agreement with a data subject.

(3) A data controller must subscribe to all the principles outlined in section 51 and not merely to parts thereof.

(4) The rights and obligations of the parties in respect of the breach of the principles outlined in section 51 are governed by the terms of any agreement between them.

Principles for electronically collecting personal information

51. (1) A data controller must have the express written permission of the data subject

Stellenbosch University http://scholar.sun.ac.za

for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

(2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.

(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.

(8) The data controller must delete or destroy all personal information which has become obsolete.

(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

CHAPTER IX

PROTECTION OF CRITICAL DATABASES

Scope of critical database protection

52. The provisions of this Chapter only apply to a critical database administrator and critical databases or parts thereof.

Identification of critical data and critical databases

53. The Minister may by notice in the *Gazette*—

(a) declare certain classes of information which is of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens to be critical data for the purposes of this Chapter; and

(b) establish procedures to be followed in the identification of critical databases for the purposes of this Chapter.

Registration of critical databases

54. (1) The Minister may by notice in the *Gazette* determine—

(a) requirements for the registration of critical databases with the Department or such other body as the Minister may specify;

(b) procedures to be followed for registration; and

(c) any other matter relating to registration.

(2) For purposes of this Chapter, registration of a critical database means recording the following information in a register maintained by the Department or by such other body as the Minister may specify:

(a) The full name, address and contact details of the critical database administrator;

(b) the location of the critical database, including the locations of component parts thereof where a critical database is not stored at a single location; and

(c) a general description of the categories or types of information stored in the critical database excluding the contents of such critical database.

Management of critical databases

55. (1) The Minister may prescribe minimum standards or prohibitions in respect of—

(a) the general management of critical databases;

(b) access to, transfer and control of critical databases;

(c) infrastructural or procedural rules and requirements for securing the integrity and authenticity of critical data;

(d) procedures and technological methods to be used in the storage or archiving of critical databases;

(e) disaster recovery plans in the event of loss of critical databases or parts thereof; and

(f) any other matter required for the adequate protection, management and control of critical databases.

(2) In respect of critical databases administered by public bodies, all regulations contemplated in subsection (1) must be made in consultation with all members of the Cabinet affected by the provisions of this Chapter: Provided that the Minister must not record information contemplated in section 54(2) if that information could reasonably compromise—

(a) the security of such databases; or

(b) the physical safety of a person in control of the critical database.

(3) This Chapter must not be construed so as to prejudice the right of a public body to perform any function authorised in terms of any other law.

Restrictions on disclosure of information

56. (1) Information contained in the register provided for in section 54 must not be disclosed to any person other than to employees of the Department who are responsible for the keeping of the register.

(2) Subsection (1) does not apply in respect of information which is disclosed—

(a) to a relevant authority which is investigating a criminal offence or for the purposes of any criminal proceedings;

(b) to government agencies responsible for safety and security in the Republic pursuant to an official request;

(c) to a cyber inspector for purposes of section 57;

(d) pursuant to sections 11 and 30 of the Promotion of Access to Information Act, 2000; or

(e) for the purposes of any civil proceedings which relate to the critical data or parts thereof.

Right of inspection

57. (1) The Director-General may, from time to time, cause audits to be performed at a critical database administrator to evaluate compliance with the provisions of this Chapter.

(2) The audit may be performed either by cyber inspectors or an independent auditor.

Non-compliance with Chapter

58. (1) Should the audit contemplated in section 57 reveal non-compliance by the critical database administrator with this Chapter, the Director-General must notify the critical database administrator thereof in writing, stating—

(a) the finding of the audit report;

(b) the action required to remedy the non-compliance; and

(c) the period within which the remedial action must be performed.

Stellenbosch University http://scholar.sun.ac.za

(2) A critical database administrator that fails to take the remedial action within the period stated in the notice is guilty of an offence.

CHAPTER X

DOMAIN NAME AUTHORITY AND ADMINISTRATION

Part 1

Establishment and incorporation of .za domain name authority

Establishment of Authority

59. A juristic person to be known as the .za Domain Name Authority is hereby established for the purpose of assuming responsibility for the .za domain name space as from a date determined by the Minister by notice in the *Gazette* and by notifying all relevant authorities.

Incorporation of Authority

60. (1) The Minister must, within 12 months of the date of commencement of this Act, take all steps necessary for the incorporation of the Authority as a company contemplated in section 21(1) of the Companies Act, 1973 (Act No. 61 of 1973).

(2) All citizens and permanent residents of the Republic are eligible for membership of the Authority and must be registered as members upon application and on payment of a nominal fee to cover the cost of registration of membership and without having to comply with any formality.

(3) For the purpose of the incorporation of the Authority a person representing the Minister and the members of Namespace ZA as at the date of application for incorporation must be deemed to be members of the Authority.

Authority's memorandum and articles of association

61. (1) The memorandum of association and articles of association of the Authority must be consistent with this Chapter and, except where this Chapter provides to the contrary, also with the Companies Act, 1973 (Act No. 61 of 1973).

(2) Notwithstanding the Companies Act, 1973, an amendment to the memorandum of association or articles of association affecting any arrangement made by any provision of this Chapter, does not have any legal force and effect unless the Minister has consented in writing to such an amendment, which consent may not be withheld unreasonably.

(3) No fee is payable in terms of the Companies Act, 1973, in respect of the reservation of the name of the company, the registration of the said memorandum and articles and the issue of the certificate to commence business.

(4) The memorandum and articles of association of the Authority must, amongst others, provide for—

(a) the rules for the convening and conducting of meetings of the Board, including the quorum required for and the minutes to be kept of those meetings;

(b) the manner in which decisions are to be made;

(c) the establishment of any division of the Authority to perform specialised functions;

(d) the establishment and functioning of committees, including a management committee;

(e) the co-opting by the Board or a committee of any person to assist the Authority or committee in the consideration of any particular matter;

(f) the preparation by the Board of an annual business plan in terms of which the activities of the Authority are planned annually;

(g) the banking and investment of funds by the Board;

(h) provisions to regulate the manner in which, and procedures whereby, expertise from any person is obtained in order to further the objects of the Authority;

(i) the determination through arbitration of any dispute concerning the interpretation of the memorandum and articles of association of the Authority;

(j) the delegation of powers and assignment of duties to directors, committees and employees: Provided that the Board may—

(i) not be divested of any power or duty by virtue of the delegation or assignment; and

(ii) vary or set aside any decision made under any delegation or in terms of any assignment;

(k) the procedures and criteria for the establishment and disestablishment of second level domains and for delegations to such domains;

(l) appeal mechanisms;

(m) the tenure of directors;

(n) the circumstances under and the manner in which a directorship is terminated;

(o) criteria for the disqualification of directors;

(p) the method of determining the allowances to be paid to directors for attending meetings; and

(q) the powers and duties of directors.

Part 2

Governance and staffing of Authority

Board of directors of Authority

62. (1) The Authority is managed and controlled by a Board of Directors consisting of nine directors, one of whom is the chairperson.

(2) The process of appointment is the following:

(a) The Minister must appoint an independent selection panel consisting of five persons, who command public respect for their fair-mindedness, wisdom and understanding of issues concerning the Internet, culture, language, academia and business, the names of whom must be placed in a notice in the *Gazette*;

(b) the Minister must invite nominations for members of the Board from the public through newspapers which have general circulation throughout the Republic, on-line news services, radio and by notice in the *Gazette*;

(c) nominations must be made to the panel established in terms of paragraph *(a)*;

(d) the panel must recommend to the Minister names of nine persons to be appointed to the Board taking into account the sectors of stakeholders listed in subsection (3)*(b)*;

(e) if the Minister is not satisfied that the recommendations of the panel comply with subsection (3) the Minister may request the panel to review its recommendations and make new ones;

(f) the Minister must appoint the members of the Board, and publish the names of those appointed in the *Gazette*;

(g) the Minister must appoint the Chairperson of the Board from among the names recommended by the panel.

(3) *(a)* The Board, when viewed collectively, must be broadly representative of the demographics of the country, including having regard to gender and disability.

(b) Sectors of stakeholders contemplated in subsection (2)*(d)* are—

(i) The existing Domain Name community;

(ii) Academic and legal sectors;

(iii) Science, technology and engineering sectors;

(iv) Labour;

(v) Business and the private sector;

(vi) Culture and language;

(vii) Public sector;

(viii) Internet user community.

(4) Directors must be persons who are committed to fairness, openness and accountability and to the objects of this Act.

Stellenbosch University http://scholar.sun.ac.za

(5) All directors serve in a part-time and non-executive capacity.

(6) Any vacancy on the Board must be filled in accordance with subsections (2) and (3).

Staff of Authority

63. (1) The chief executive officer of the Authority appointed by the Board must perform any work incidental to the functions of the Authority.

(2) The chief executive officer must be assisted by staff appointed by the Board.

(3) The Board must determine the conditions of service, remuneration and service benefits of the chief executive officer and the staff.

(4) If the chief executive officer is for any reason unable to perform his or her functions, the Board may designate a person in the service of the Authority to act as the acting chief executive officer until the chief executive officer is able to resume office.

Part 3

Functions of Authority

Licensing of registrars and registries

64. (1) No person may update a repository or administer a second level domain unless such person is licensed to do so by the Authority.

(2) An application to be licensed as a registrar or registry must be made in the prescribed manner and subject to the prescribed fees.

(3) The Authority must apply the prescribed conditions and criteria when evaluating an application referred to in subsection (2).

Functions of Authority

65. (1) The Authority must—

(a) administer and manage the .za domain name space;

(b) comply with international best practice in the administration of the .za domain name space;

(c) license and regulate registries;

(d) license and regulate registrars for the respective registries; and

(e) publish guidelines on—

(i) the general administration and management of the .za domain name space;

(ii) the requirements and procedures for domain name registration; and

(iii) the maintenance of and public access to a repository,

with due regard to the policy directives which the Minister may make from time to time by notice in the *Gazette*.

(2) The Authority must enhance public awareness on the economic and commercial benefits of domain name registration.

(3) The Authority—

(a) may conduct such investigations as it may consider necessary;

(b) must conduct research into and keep abreast of developments in the Republic and elsewhere on the domain name system;

(c) must continually survey and evaluate the extent to which the .za domain name space meets the needs of the citizens of the Republic; and

(d) may, from time to time, issue information on the registration of domain names in the Republic.

(4) The Authority may, and must when so requested by the Minister, make recommendations to the Minister in relation to policy on any matter relating to the .za domain name space.

(5) The Authority must continually evaluate the effectiveness of this Act and things done in terms thereof towards the management of the .za domain name space.

(6) The Authority may—

(a) liaise, consult and co-operate with any person or other authority; and

(b) appoint experts and other consultants on such conditions as the Authority may determine.

(7) The Authority must respect and uphold the vested rights and interests of parties that were actively involved in the management and administration of the .za domain name space at the date of its establishment: Provided that—

(a) such parties must be granted a period of six months during which they may continue to operate in respect of their existing delegated sub-domains; and

(b) after the expiry of the six-month period, such parties must duly apply to be licensed registrars and registries as provided for in this Part.

Part 4

Finances and reporting

Finances of Authority

66. (1) All money received by the Authority must be deposited in a banking account in the name of the Authority with a bank established under the Banks Act, 1990 (Act No. 94 of 1990), or a mutual bank established under the Mutual Banks Act, 1993 (Act No. 124 of 1993).

(2) The chief executive officer is the accounting officer of the Authority and must ensure that—

(a) proper record of all the financial transactions, assets and liabilities of the Authority are kept; and

(b) as soon as possible, but not later than three months after the end of a financial year, accounts reflecting the income and expenditure of the Authority and a balance sheet of the assets and liabilities of the Authority as at the end of that financial year are prepared and submitted to the Board and Minister.

(3) The Authority is funded from—

(a) the capital invested in or lent to the Authority;

(b) money appropriated by Parliament for that purpose;

(c) income derived from the sale or other commercial exploitation of its licenses, approvals, products, technology, services or expertise in terms of this Act;

(d) loans raised by the Authority;

(e) the proceeds of any sale of assets;

(f) income or interest earned on the Authority's cash balances or on money invested by it; and

(g) money received by way of grant, contribution, donation or inheritance from any source inside or outside the Republic.

(4) The funds of the Authority must be utilised to meet the expenditure incurred by the Authority in connection with its functioning, business and operations in terms of this Act.

(5) *(a)* The money may be so utilised only as provided for in a statement of the Authority's estimated income and expenditure, that has been approved by the Minister.

(b) Money received by way of grant, contribution, donation or inheritance in terms of subsection (3)*(g)*, must be utilised in accordance with any conditions imposed by the grantor, contributor, donor or testator concerned.

(6) *(a)* The Board must in each financial year, at a time determined by the Minister, submit to the Minister for approval a statement of the Authority's estimated income and expenditure for the next financial year.

(b) The Board may at any time during the course of a financial year, submit a supplementary statement of estimated income and expenditure of the Authority for that financial year, to the Minister for approval.

(c) The Minister may grant the approval of the statement referred to in paragraph *(a)*, with the agreement of the Minister of Finance.

(d) The Authority may not incur any expenditure in excess of the total amount approved under paragraph *(c)*.

(7) The Board may establish a reserve fund for any purpose that is connected with the Authority's functions under this Act and has been approved by the Minster, and may allocate to the reserve fund the money that may be made available for the purposes in the

Stellenbosch University http://scholar.sun.ac.za

statement of estimated income and expenditure or supplementary statement contemplated in subsection (6).

(8) To the extent that the Authority is provided with start-up capital by the State, the Authority may, at the election of the Minister of Finance, be made subject to the Public Finance Management Act, (Act No. 1 of 1999), until such time as the Authority, to the satisfaction of the Minister of Finance, becomes self-sustaining through the alternative sources of revenue provided for in subsection (3).

Reports

67. As soon as practicable after the end of every financial year, the Board must submit a report on its activities during that year to the Minister who must table that report in Parliament.

Part 5

Regulations

Regulations regarding Authority

68. The Authority may, with the approval of the Minister, make regulations regarding—

(a) the requirements which registries and registrars must meet in order to be licensed, including objective standards relating to operational accuracy, stability, robustness and efficiency;

(b) the circumstances and manner in which registrations may be assigned, registered, renewed, refused, or revoked by the registries with due regard to the express recognition of the right of groups and members of groups within the Republic to identify with, use or communicate cultural, linguistic, geographical, indigenous or any other expressions of heritage including any visual or audible elements or attributes thereof;

(c) pricing policy;

(d) provisions for the restoration of a domain name registration and penalties for late payments;

(e) the terms of the domain name registration agreement which registries and registrars must adopt and use in registering domain names, including issues in respect of privacy, consumer protection and alternative dispute resolution;

(f) processes and procedures to avoid unfair and anti-competitive practices, including bias to, or preferential treatment of actual or prospective registrants, registries or registrars, protocols or products;

(g) requirements to ensure that each domain name contains an administrative and technical contact;

(h) the creation of new sub-domains;

(i) procedures for ensuring monitoring of compliance with the provisions of this Act and the regulations provided for in this Chapter, including regular .za domain name space technical audits;

(j) such other matters relating to the .za domain name space as it may be necessary to prescribe to achieve the objectives of this Chapter; and

(k) policy to be applied by the Authority.

Part 6

Alternative dispute resolution

Alternative dispute resolution

69. (1) The Minister, in consultation with the Minister of Trade and Industry, must make regulations for an alternative mechanism for the resolution of disputes in respect of the .za domain name space.

(2) The regulations must be made with due regard to existing international precedent.

(3) The regulations may prescribe—

(a) procedures for the resolution of certain types of disputes determined in the regulations and which relate to a domain name registration;

(b) the role which the Authority must fulfil in administering the dispute resolution procedure;

(c) the appointment, role and function of dispute resolution adjudicators;

(d) the procedure and rules which must be followed in adjudicating disputes;

(e) unlawful actions or activities in respect of domain names, distinguishing between criminal and civil liability;

(f) measures to prevent unlawful actions or activities with respect to domain names;

(g) the manner, costs of and time within which a determination must be made;

(h) the implementation of determinations made in terms of the dispute resolution procedure;

(i) the limitation of liability of registrars and registries for implementing a determination; and

(j) the enforcement and publication of determinations.

CHAPTER XI

LIMITATION OF LIABILITY OF SERVICE PROVIDERS

Definition

70. In this Chapter, "service provider" means any person providing information system services.

Recognition of representative body

71. (1) The Minister may, on application by an industry representative body for service providers by notice in the *Gazette*, recognise such body for purposes of section 72.

(2) The Minister may only recognise a representative body referred to in subsection (1) if the Minister is satisfied that—

(a) its members are subject to a code of conduct;

(b) membership is subject to adequate criteria;

(c) the code of conduct requires continued adherence to adequate standards of conduct; and

(d) the representative body is capable of monitoring and enforcing its code of conduct adequately.

Conditions for eligibility

72. The limitations on liability established by this Chapter apply to a service provider only if—

(a) the service provider is a member of the representative body referred to in section 71; and

Stellenbosch University http://scholar.sun.ac.za

(*b*) the service provider has adopted and implemented the official code of conduct of that representative body.

Mere conduit

73. (1) A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider—

(*a*) does not initiate the transmission;

(*b*) does not select the addressee;

(*c*) performs the functions in an automatic, technical manner without selection of the data; and

(*d*) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place—

(*a*) for the sole purpose of carrying out the transmission in the information system;

(*b*) in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and

(*c*) for a period no longer than is reasonably necessary for the transmission.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

Caching

74. (1) A service provider that transmits data provided by a recipient of the service via an information system under its control is not liable for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other recipients of the service upon their request, as long as the service provider—

(*a*) does not modify the data;

(*b*) complies with conditions on access to the data;

(*c*) complies with rules regarding the updating of the data, specified in a manner widely recognised and used by industry;

(*d*) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain information on the use of the data; and

(*e*) removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 77.

(2) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

Hosting

75. (1) A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider—

(*a*) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of a third party; or

(*b*) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and

(*c*) upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its services, including on its web sites in locations accessible to the public, the name, address, phone number and e-mail address of the agent.

(3) Notwithstanding this section, a competent court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

(4) Subsection (1) does not apply when the recipient of the service is acting under the authority or the control of the service provider.

Information location tools

76. A service provider is not liable for damages incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider—

(*a*) does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;

(*b*) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;

(*c*) does not receive a financial benefit directly attributable to the infringing activity; and

(*d*) removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to such data message, infringes the rights of a person.

Take-down notification

77. (1) For the purposes of this Chapter, a notification of unlawful activity must be in writing, must be addressed by the complainant to the service provider or its designated agent and must include—

(*a*) the full names and address of the complainant;

(*b*) the written or electronic signature of the complainant;

(*c*) identification of the right that has allegedly been infringed;

(*d*) identification of the material or activity that is claimed to be the subject of unlawful activity;

(*e*) the remedial action required to be taken by the service provider in respect of the complaint;

(*f*) telephonic and electronic contact details, if any, of the complainant;

(*g*) a statement that the complainant is acting in good faith;

(*h*) a statement by the complainant that the information in the take-down notification is to his or her knowledge true and correct; and

(2) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts is liable for damages for wrongful take-down.

(3) A service provider is not liable for wrongful take-down in response to a notification.

No general obligation to monitor

78. (1) When providing the services contemplated in this Chapter there is no general obligation on a service provider to—

(*a*) monitor the data which it transmits or stores; or

(*b*) actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to section 14 of the Constitution, prescribe procedures for service providers to—

(*a*) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and

(*b*) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

Savings

79. This Chapter does not affect—

(*a*) any obligation founded on an agreement;

Stellenbosch University http://scholar.sun.ac.za

(b) the obligation of a service provider acting as such under a licensing or other regulatory regime established by or under any law;
(c) any obligation imposed by law or by a court to remove, block or deny access to any data message; or
(d) any right to limitation of liability based on the common law or the Constitution.

CHAPTER XII

CYBER INSPECTORS

Appointment of cyber inspectors

80. (1) The Director-General may appoint any employee of the Department as a cyber inspector empowered to perform the functions provided for in this Chapter.

(2) A cyber inspector must be provided with a certificate of appointment signed by or on behalf of the Director-General in which it is stated that he or she has been appointed as a cyber inspector.

(3) A certificate provided for in subsection (2) may be in the form of an advanced electronic signature.

(4) When a cyber inspector performs any function in terms of this Act, he or she must—
(a) be in possession of a certificate of appointment referred to in subsection (2); and
(b) show that certificate to any person who—
(i) is subject to an investigation or an employee of that person; or
(ii) requests to see the certificate.

(5) Any person who—
(a) hinders or obstructs a cyber inspector in the performance of his or her functions in terms of this Chapter; or
(b) falsely holds himself or herself out as a cyber inspector,
is guilty of an offence.

Powers of cyber inspectors

81. (1) A cyber inspector may—
(a) monitor and inspect any web site or activity on an information system in the public domain and report any unlawful activity to the appropriate authority;
(b) in respect of a cryptography service provider—
(i) investigate the activities of a cryptography service provider in relation to its compliance or non-compliance with the provisions of this Act; and
(ii) issue an order in writing to a cryptography service provider to comply with the provisions of this Act;
(c) in respect of an authentication service provider—
(i) investigate the activities of an authentication service provider in relation to its compliance or non-compliance with the provisions of this Act;
(ii) investigate the activities of an authentication service provider falsely holding itself, its products or services out as having been accredited by the Authority or recognised by the Minister as provided for in Chapter VI;
(iii) issue an order in writing to an authentication service provider to comply with the provisions of this Act; and
(d) in respect of a critical database administrator, perform an audit as provided for in section 57.

(2) Any statutory body, including the South African Police Service, with powers of inspection or search and seizure in terms of any law may apply for assistance from a cyber inspector to assist it in an investigation: Provided that—

(a) the requesting body must apply to the Department for assistance in the prescribed manner; and
(b) the Department may authorise such assistance on certain conditions.

Power to inspect, search and seize

82. (1) A cyber inspector may, in the performance of his or her functions, at any reasonable time, without prior notice and on the authority of a warrant issued in terms of section 83(1), enter any premises or access an information system that has a bearing on an investigation and—
(a) search those premises or that information system;
(b) search any person on those premises if there are reasonable grounds for believing that the person has personal possession of an article, document or record that has a bearing on the investigation;
(c) take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation;
(d) demand the production of and inspect relevant licences and registration certificates as provided for in any law;
(e) inspect any facilities on the premises which are linked or associated with the information system and which have a bearing on the investigation;
(f) have access to and inspect the operation of any computer or equipment forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to suspect is or has been used in connection with any offence;
(g) use or cause to be used any information system or part thereof to search any data contained in or available to such information system;
(h) require the person by whom or on whose behalf the cyber inspector has reasonable cause to suspect the computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system to provide him or her with such reasonable technical and other assistance as he or she may require for the purposes of this Chapter; or
(i) make such inquiries as may be necessary to ascertain whether the provisions of this Act or any other law on which an investigation is based, have been complied with.

(2) A person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence.

(3) The Criminal Procedure Act, 1977 (Act No. 51 of 1977), applies with the necessary changes to searches and seizures in terms of this Act.

(4) For purposes of this Act, any reference in the Criminal Procedure Act, 1977, to "premises" and "article" includes an information system as well as data messages.

Obtaining warrant

83. (1) Any magistrate or judge may, upon a request from a cyber inspector but subject to the provisions of section 25 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), issue a warrant required by a cyber inspector in terms of this Chapter.

(2) For the purposes of subsection (1), a magistrate or judge may issue a warrant where—
(a) an offence has been committed within the Republic;
(b) the subject of an investigation is—
(i) a South African citizen or ordinarily resident in the Republic; or
(ii) present in the Republic at the time when the warrant is applied for; or
(c) information pertinent to the investigation is accessible from within the area of jurisdiction of the court.

(3) A warrant to enter, search and seize may be issued at any time and must—
(a) identify the premises or information system that may be entered and searched; and

Stellenbosch University http://scholar.sun.ac.za

(*b*) specify which acts may be performed thereunder by the cyber inspector to whom it is issued.

(4) A warrant to enter and search is valid until—

(*a*) the warrant has been executed;

(*b*) the warrant is cancelled by the person who issued it or in that person's absence, by a person with similar authority;

(*c*) the purpose for issuing it has lapsed; or

(*d*) the expiry of one month from the date on which it was issued.

(5) A warrant to enter and search premises may be executed only during the day, unless the judge or magistrate who issued it, authorises that it may be executed at any other time.

Preservation of confidentiality

84. (1) Except for the purpose of this Act or for the prosecution of an offence or pursuant to an order of court, a person who has, pursuant to any powers conferred under this Chapter, obtained access to any information may not disclose such information to any other person.

(2) Any person who contravenes subsection (1) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding six months.

CHAPTER XIII

CYBER CRIME

Definition

85. In this Chapter, unless the context indicates otherwise—

"access" includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.

Unauthorised access to, interception of or interference with data

86. (1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

(5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

Computer-related extortion, fraud and forgery

87. (1) A person who performs or threatens to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions, is guilty of an offence.

(2) A person who performs any of the acts described in section 86 for the purpose of obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic, is guilty of an offence.

Attempt, and aiding and abetting

88. (1) A person who attempts to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.

(2) Any person who aids and abets someone to commit any of the offences referred to in sections 86 and 87 is guilty of an offence and is liable on conviction to the penalties set out in section 89(1) or (2), as the case may be.

Penalties

89. (1) A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.

(2) A person convicted of an offence referred to in section 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.

CHAPTER XIV

GENERAL PROVISIONS

Jurisdiction of courts

90. A court in the Republic trying an offence in terms of this Act has jurisdiction where—

(*a*) the offence was committed in the Republic;

(*b*) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

(*c*) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or

(*d*) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

Saving of common law

91. This Chapter does not affect criminal or civil liability in terms of the common law.

Repeal of Act 57 of 1983

92. The Computer Evidence Act, 1983, is hereby repealed.

Limitation of liability

93. Neither the State, the Minister, nor any employee of the State is liable in respect of any act or omission in good faith and without gross negligence in performing a function in terms of this Act.

Regulations

94. The Minister may make regulations regarding any matter that may or must be prescribed in terms of this Act or any matter which it is necessary or expedient to prescribe for the proper implementation or administration of this Act.

Stellenbosch University http://scholar.sun.ac.za

Short title and commencement

95. This Act is called the Electronic Communications and Transactions Act, 2002, and comes into operation on a date fixed by the President by proclamation in the *Gazette*.

SCHEDULE 1

(see section 4(3))

Item	Column A	Column B
1.	Wills Act, 1953 (Act No. 7 of 1953)	11, 12, 13, 14, 15, 16, 18, 19 and 20
2.	Alienation of Land Act, 1981 (Act No. 68 of 1981)	12 and 13
3.	Bills of Exchange Act, 1964 (Act No. 34 of 1964)	12 and 13
4.	Stamp Duties Act, 1968 (Act No. 77 of 1968)	11, 12, 14

Stellenbosch University http://scholar.sun.ac.za

SCHEDULE 2

(see section 4(4))

1.	An agreement for alienation of immovable property as provided for in the Alienation of Land Act, 1981 (Act No. 68 of 1981).
2.	An agreement for the long-term lease of immovable property in excess of 20 years as provided for in the Alienation of Land Act, 1981 (Act No. 68 of 1981).
3.	The execution, retention and presentation of a will or codicil as defined in the Wills Act, 1953 (Act No. 7 of 1953).
4.	The execution of a bill of exchange as defined in the Bills of Exchange Act, 1964 (Act No. 34 of 1964).

Stellenbosch University http://scholar.sun.ac.za

BRONNELYS

About ISPA. (2002). *Internet Service Providers Association*. Afgelaai 17 Desember 2002 van http://www.ispa.org.za/about.htm.

About WIPO. (2002). *World Intellectual Property Organization*. Afgelaai 27 Januarie 2003 van http://www.wipo.org/about-wipo/en/gib.htm.

Abrea, E.M. (2002 Maart). Famed hacker comes clean. *News24*. Afgelaai 11 Desember 2002 van http://www.news24.com/News24/Technology/Infotech/0,1113,2-13-45_1266458,00.html.

Alberts, A. de W. (2001). Internet Regulation. In R. Buys (Ed.) *Cyberlaw@Sa: The Law of the Internet in South Africa* (pp. 393-421). Pretoria, Van Schaik.

All About the Internet Society. (2002). *Internet Society (ISOC)*. Afgelaai 5 Desember 2002 van http://www.isoc.org/isoc/.

Altschull, J.H. (1990). *From Milton to McLuhan: The Ideas Behind American Journalism.* New York: Longman.

An International Survey of the Internet. (2002). *ACNielson NetWatch*. Afgelaai 2 Desember 2002 van http://www.acnielsen.com/products/reports/netwatch/index.htm

Approved Providers for Uniform Domain-Name Dispute-Resolution Policy. (Maart 2002). *ICANN*. Afgelaai 14 September 2002 van http://www.icann.org/dndr/udrp/approved-providers.htm.

Baker, S. (1999). Taming the Wild, WIld Web: Without strong laws, the Net's growth wil be stunted. *Business Week,* 4 Okt. 1999: 92-94.

Barlow, J. (2001, Maart). Jurisdiction and You - Yahoo! *The Internet Law Journal.* Afgelaai 19 Oktober 2002 van http://www.internetlawjournal.com/content/litigation-article03080102.htm.

Bolmer, N.A. (2002, September). When Push Comes to Shove: Who Controls Where and How We Surf the Web. *The Internet Law Journal.* Afgelaai 19 Oktober 2002 van http://www.internetlawjournal.com/content/iparticle09010201.htm.

Buys, R. (2002). *Cyperlaw@SA: Top100 FAQs.* VirtualBook, Observatory, Cape Town 2002.

Stellenbosch University http://scholar.sun.ac.za

Buys, R. (2001). Freedom of expression and the Internet. In R. Buys (Ed.) *Cyberlaw@Sa: The Law of the Internet in South Africa* (pp. 329-362). Pretoria, Van Schaik.

Carny, D. *et al.*(2000). Whose Net is it, anyway? *Business Week,* 31 July 2000: 58.

Cerf, V. (1993). How the Internet Came to Be. Afgelaai 6 Junie 2001 van http:///www.zakon.rog/robert/internet/timeline/.

Comments on the ECT Bill by Namespace ZA. (2002). *Namespace ZA*. Afgelaai 17 Desember 2002 van http://www.namespace.org.za.

Constitution of the Internet Service Providers' Association. (2002, September). *Internet Service Providers' Association*. Afgelaai 17 Desember 2002 van http://www.ispa.org.za.

Convention on Cybercrime. (2001). *Council of Europe*. Afgelaai 27 November 2002 van http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm

De Beer, A.S. & Diederiechs, P. (1998). Newspapers The Fourth Estate: A cornerstone of democracy. In De Beer, A.S. (Ed.). 1998. *Mass media for the Nineties - The South African Handbook of Mass Communication* (tweede uitgawe). Pretoria: J.L. van Schaik: 87.

De Bruin, P. (2003). Nuwe wet hou reuse-koste in. Sake Burger, 3 Februarie 2003: S11.

De Villiers, R. (2000). Copyright and the Internet. *Legalnet.* Afgelaai 10 November 2002 van http://www.legalnet.co.za/cyberlaw/frpreface.htm.

De Villiers, R. (2001). Copyright and the Internet. In R. Buys (Ed.) *Cyberlaw@SA: The Law of the Internet in South Africa* (pp. 37-67). Pretoria, Van Schaik.

De Wet, P. (2002, Julie). Mbeki to sign ECT Bill tomorrow. *ITWet*. Afgelaai 8 Desember 2002 van http://www.itweb.co.za/sections/quickprint/print.asp?StoryID=125300.

Domeinname vir 'n makliker lewe. (2002). Taking e-commerce to the people. Department of Education. Media24 Promosie-bylae, Desember 2002: 2.

Dudley, G. (2002). Kyk watse hoede dra die kuberkrakers: Netwerkindringers ontwyk 'n misdaadprofiel deur bestendig onbestendig te bly. Finansies & Tegniek, 25 September 2002: 60.

ECT Bill. (2002). *Republic of South Africa.* Creda Communications, 2002: 39-41.

Stellenbosch University http://scholar.sun.ac.za

Electronic Communications and Transactions Act No 25 of 2002. (2002). *Government Gazette, Republic of South Africa*. (Vol 446, pp. 26-76). Cape Town.

Ferreira, T. (2002). Jong Brasiliane saai chaos in SA internetwerwe. Die Burger, 28 November 2002: 3.

Ferreira, T. (2002). Jong kuberkraker verwoes Suid-Afrikaanse webwerwe. Die Burger, 26 Oktober 2002: 1.

Franze, R. (2000 November). ICANN: What's In Store For Its Future? *The Internet Law Journal*. Afgelaai 10 Desember 2002 van http://www.internetlawjournal.com/content/iparticle11140002.htm.

Free Kevin Mitnick: The Official Kevin Mitnick Site. (2002). Afgelaai 26 November 2002 van http://www.kevinmitnick.com/

Froomkin, A.M. (2002). An Introduction to the "governance" of the Internet. Afgelaai 29 Augustus 2002 van http://www.law.miami.edu/~froomkin/seminar/ilsx.htm.

Gordon, B. (2001). Internet Criminal Law. In R. Buys (Ed.) *Cyberlaw@Sa: The Law of the Internet in South Africa* (pp. 423-447). Pretoria, Van Schaik.

Hameed, I. (2002). Understanding the Internet and the WWW. *About.com*. Afgelaai 28 November 2002 van http://internet.about.com/library/aa_internet_071002.htm.

How Many Online? (2002). *NUA*. Afgelaai 17 November 2002 van http://www.nua.ie/surveys/how_many_online/index.html.

Internet Access: At Home or At Work? (2002). *ACNielsen NetWatch*. Afgelaai 2 Desember van http://www.acnielsen.com/products/reports/netwatch/pg4.htm

Internet User Survey #2. (1999). *Survey.net*. Afgelaai 18 November 2002 van http://www.survey.net/inet2r.html.

Jansen, J. (2002). A new era for e-commerce in South Africa. *De Rebus*. Afgelaai 14 Desember 2002 van http://www.derebus.org.za/archives/2002Oct/articles/E-commerce.htm.

Kok, L. (2002). Paneel sal za-naam bestuur. *SakeBurger*. 22 November 2002: S7.

Stellenbosch University http://scholar.sun.ac.za

Lawrie, M. (1990). Afgelaai 5 November 2002 van http://www2.frd.ac.za/uninet/history/zacleard.htm.

Lawrie, M. (1997). The history of the Internet in South Africa - How it began. Afgelaai 5 November 2002 van http://apies.frd.ac.za/uninet/history/.

Leading the Web to its Full Potensial. (2002). The World Wide Web Consortium. Afgelaai 5 Nomvember 2002 van http://www.w3.org/.

Leiner, B.M., et al. (2000, Augustus). A Brief History of the Internet. *The Internet Society*. Afgelaai 6 Junie 2001 van http://www.isoc.org/internet/history/brief.html.

Levine, J. (2001). The Cybercops Are Coming - But Whom Will They Serve? *Columbian Journalism Review*, Januarie/Februarie 2001: 66.

Louw, B. (2003). Stryd oor domeinname: SA in hande van Yank-maatskappy. Die Burger, 2 Januarie 2003: 3.

Lyman, J. (2001 Februarie). UN Calls For International Domain Name Rules. *NewsFactor Network*. Afgelaai 14 Desember 2002 van http://www.newsfactor.com/perl/story/7668.html.

Lyman, J. (2001 Februarie). Time Warner Wins Harry Potter Domain Name. *NewsFactor Network*. Afgelaai 14 Desember 2002 van http://www.newsfactor.com/perl/story/6264.html.

McDonald, T. (2001 September). UN Demands Stronger Rules on Global Cybersquatting. *NewsFactor Network*. Afgelaai 14 Desember 2002 van http://www.newsfactor.com/perl/story/13299.html.

Meiring, R. (2002). Petition to the President regarding the Electronic Commuinications en Transactions Bill (BB-2002). *Electronic Communications and Transactions Bill: Unofficial Information Repository*. Afgelaai 30 November 2002 van http://www.ectbill.co.za/petition.asp.

Moses, M. (1999). Internet Demographics. *New Media Lab. Journalism & Media Studies Department: Rhodes University*. Afgelaai 17 November 2002 van http://nml.ru.ac.za/carr/margot/index.html.

Stellenbosch University http://scholar.sun.ac.za

Muhlberg, H. (2002). Never say never! *De Rebus*. Afgelaai 14 Desember 2002 van http://www.derebus.org.za/scripts/derebus_s.pl?ID=44967&index=200208_articles&hitID=0 .

Namespace ZA. (2002). *Namespace ZA Homepage.* Afgelaai 17 Desember 2002 van www.namemspace.org.za.

National Arbitration Forum. (2002). Decision: South African Airways (Pty.) Limited v. Vern Six. Claim Number: FA0204000109385. Afgelaai 13 Augustus van http://www.neverflysaa.com.

National Arbitration Forum. (2002). *National Arbitration Forum*. Afgelaai 14 Augustus 2002 van http://www.arbforum.com/domains/.

Niemczyk, J. (1999). International Internet: A look inside. *MSCI Department, Virginia Tech, USA.* Afgelaai op 29 Augustus 2002 van http://www.chem.vt.edu/chem-dept/dessy/honors/papers/niemczyk.html.

Nuwe era ingelui in wêreld-elektronika. (2002). Taking e-commerce to the people. Department of Education. Media24 Promosie-bylae, Desember 2002: 2.

Online Intellectual Property Survey. (2002). *Survey.net*. Afgelaai 18 November 2002 van http://www.survey.net/ip0r.html.

Opperman, C.P. (2000 Julie). Cyberlaw: Internet Law in South Africa. *Legalnet.* Afgelaai 22 Mei 2002 van http://www.legalnet.co.za/cyberlaw/index.htm.

Polak, V.L., Miller, P.A. & Jinnett, J. (2000 Augustus). The Legal Risks of Trademarks as Internet Search Terms, *The Internet Law Journal*. Afgelaai 9 Oktober 2002 van http://www.internetlawjournal.com/content/iparticle08010001.htm

Perritt, H.H. Jr. (1996). *Law and The Information Superhighway*. The Journal of Information, Law and Technology (JILT). Afgelaai 23 Desember 2002 van http://elj,warwick.ac.uk/elj/jilt/bookrev/3waelde/

Stellenbosch University http://scholar.sun.ac.za

Rademeyer, C. (2003). Regsgeding vuurproef vir vryheid op internet. Die Burger, 13 Januarie 2003: 8.

RAND's History: 50 Years of Service to the Nation. (2001). *RAND*. Afgelaai 27 November 2002 van http://www.rand.org/history/

SAPA. Website flies in face of SAA. News24.com. Afgelaai 28 Januarie 2002 van http://www.news24.co.za/contentDisply/level4Article/0,1113,2-1134_1136331,00.html.

Sekerheid van groot belang vir sukses. (2002). Taking e-commerce to the people. Department of Education. Media24 Promosie-bylae, Desember 2002: 3

Silber, M. (2000 Februarie). Advisory 1: Trade marks and domain names. *ISPA (Internet Service Providers Association)*. Afgelaai 2 Desember 2002 van www.ispa.org.za.

Six, V. (2002). www.neverflysaa.com Home Page. Afgelaai 13 Augustus 2002 van http://www.neverflysaa.com.

Smith, G.J.H. (1996). *Internet Law and Regulation*. The Journal of Information, Law and Technology (JILT). Afgelaai 23 Desember 2002 van http://elj,warwick.ac.uk/ elj/jilt/bookrev/3lockett/.

Some facts about TENET. (2002). *TENET Home Page.* Afgelaai 23 Desember 2002 van http://www.tenet.ac.za.

South African Airway (Pty.) Limited v. Vern Six.(2002). *National Abritration Forum*. Afgelaai 13 Augustus 2002 van http://www.neverflysaa.com.

South Africa Online: User Survey 1997. (1997). *South Africa Online, House of SYNERGY.* Afgelaai 17 November 2002 van http://www.southafrica.co.za/survey_one/.

South African Usage. (2002). *Internet Solutions.* Afgelaai 17 November 2002 van http://www.is.co.za/webstats/?Quickprint=1.

Stellenbosch University http://scholar.sun.ac.za

Stein, L. & Kidd, D. (2000). The Future of Openness on the Internet. *Media Alliance*. Afgelaai 27 November 2002 van http://www.media-alliance.org/mediafile/19-3/openaccess.html.

Tagoe, C. (2000). Internet Domain Disputes Under ICANN's Uniform Dispute Resolution Policy. *The Internet Law Journal*. Afgelaai 10 September 2002 van http://www.internetlawjournal.com/content/iparticle09110001.htm.

Temme, T. (1997). Principles of Human Communication. *Fachhochschule Osnabrück University of Applied Sciences*. Afgelaai 27 November 2002 van http://www.wi.fh-osnabrueck.de/tutor/mk/comunic/comprinc/index.htm.

The 1998 South African Web User Survey. (1998). *South Africa Online, The House of SYNERGY*. Afgelaai 17 November 2002 van http://www.thos.co.za/news/240498_sao.html.

The 3rd South African Web User Survey. (1999). *South Africa Online, The House of SYNERGY*. Afgelaai 17 November 2002 van http://www.southafrica.co.za/survey/.

The Constitution of the South African Chapter. (2002). *ISOC ZA*. Afgelaai 17 Desember 2002 van http://www.isoc.org.za/about.asp.

The draft international Convention. (2001). *Council of Europe*. Afgelaai 27 November 2002 van http://www.coe.int/T/E/Communication_and_Research/Press/Theme_Files/Cybercr…/e_projconvention.asp.

The Internet Corporation for Assigned Names and Numbers. (2002). *ICANN Home Page* Afgelaai 14 Augustus 2002 van http://www.icann.org/.

USA Background. (2002). *Universal Service Agency Homepage*. Afgelaai 17 Desember 2002 van http://www.usa.org.za/background.html.

Vegter, I. and De Wet, P. (2002). *Laying down cyber law*. IT Web Brainstorm, March 2002.

Viljoen. M, Du Plessis, GM and Vivier, G. (2001)). Trademarks, domain names and patents. In R. Buys (Ed.) *Cyberlaw@Sa: The Law of the Internet in South Africa* (pp. 71-95). Cape Town, Van Schaik.

Stellenbosch University http://scholar.sun.ac.za

Voordele van elektroniese handtekening. (2002). Taking e-commerce to the people. Department of Education. Media24 Promosie-bylae, Desember 2002: 3.

Who is not using the Internet? (2002). *ACNielsen NetWatch*. Afgelaai 2 Desember 2002 van http://www.acnielsen.com/products/reports/netwatch/pg3.htm.

Whose Net is it, anyway? *Newsweek* 31 Julie 2000: p. 34.

Wkj? En M-Web Afrikaans slaan vuis.*watkykjy?* Afgelaai 29 Januarie 2002 van http://www.watkykjy.co.za/wkj14/snot05.html.

World Wide Wox: More South Africans to get online this year. (2002). *NUA*. Afgelaai 17 November 2002 van http://wwwnua.ie/surveys/indes.cgi?f=VS&art_id=905358016&rel=true.